

Codes in the Damerau Distance for Deletion and Adjacent Transposition Correction

Ryan Gabrys*, Eitan Yaakobi[‡], and Olgica Milenkovic*

*ECE Department, University of Illinois, Urbana-Champaign [‡]Technion University

Abstract—Motivated by applications in DNA-based storage, we introduce the new problem of code design in the Damerau metric. The Damerau metric is a generalization of the Levenshtein distance which, in addition to deletions, insertions and substitution errors also accounts for adjacent transposition edits. We first provide constructions for codes that may correct either a single deletion or a single adjacent transposition and then proceed to extend these results to codes that can simultaneously correct a single deletion and multiple adjacent transpositions. We conclude with constructions for joint block deletion and adjacent block transposition error-correcting codes.

I. INTRODUCTION

The edit distance is a measure of similarity between two strings evaluated based on the minimum number of operations required to transform one string into the other. If the operations are confined to symbol deletions, insertions and substitutions, the distance of interest is the Levenshtein (edit) distance [15]. The Levenshtein distance has found numerous applications in bioinformatics, where a weighted version of this metric is used to assess the similarity of DNA strings and reconstruct phylogenetic trees [14], and natural language processing, where the distance is used to model spelling errors and provide automated word correction [4].

In parallel to the work on developing efficient algorithms for computing the edit distance and performing alignments of large number of strings, a long line of results were reported on the topic of designing codes for this distance function. Codes in the edit distance are of particular importance for communication in the presence of synchronization errors, a type of error encountered in almost all modern storage and data transmission systems. Classical derivations of upper bounds on code sizes by Levenshtein [15] and single deletion-correcting code constructions by Varshamov and Tenengoltz [21], [22] have established the framework for studying many challenging problems in optimal code design for this metric [3], [7], [12], [18], [20].

The Damerau distance is an extension of the Levenshtein distance that also allows for edits of the form of adjacent symbol transpositions [4]. Despite the apparent interest in coding for edit channels, the problem of designing codes in the Damerau distance was not studied before. A possible reason for this lack of interest in the Damerau distance may be attributed to the fact that not many practical channel models involve adjacent transposition errors, and even if they do so, they tend not to allow for user-selected messages. Our motivating application for studying codes in the Damerau distance is the emerging paradigm of DNA-based storage [2], [6], [10], [25], [26]. In DNA-based storage systems, media degradation arises due to DNA aging caused by metabolic and hydrolytic processes, or

more precisely, by exposure to standard or increased level radiation, humidity, and high temperatures. As an example, human cellular DNA undergoes anywhere between 10-50 breakages in a cell cycle [23]. These DNA breakages or symbol/block deletions result in changed structures of the string: If a string breaks in two places, which is the most likely scenario, either the sequence reattaches itself without resulting in structural damage, reattaches itself in the opposite direction, resulting in what is called a *reversal error*, or the broken string degrades, resulting in a bursty (block) deletion; if a string breaks in three positions, which is the second most likely breakage scenario, either the adjacent broken blocks exchange positions or one or both block disintegrate leading to a bursty deletion. It is the latter scenario that motivates the study of channels in which adjacent blocks of symbols may be exchanges or individual blocks deleted. It is straightforward to see that this editing scenario corresponds to a “block version” of the Damerau editing process. The block editing process is hard to analyze directly, so we first study the symbol-level Damerau editing process and then proceed to analyze the block model. Also, for simplicity of exposition, we focus our attention on deletion and adjacent transposition errors and delegate the more complex analysis of all four edit operations to future work.

Our contributions are two-fold. We introduce the Damerau distance code design problem, and describe the first known scheme for correcting one deletion *or* one adjacent transposition. The scheme has near-optimal redundancy. We then proceed to extend and generalize this construction so as to obtain codes capable of correcting one deletion *and* one adjacent transposition that also have near-optimal redundancy. Our results also shed light on the new problems of *mismatched* Varshamov-Tenengoltz (VT) decoding and run length limited VT codes. Second, we describe significantly more involved code constructions for correction of multiple adjacent transposition errors and proceed to introduce codes capable of correcting a block deletion and adjacent block transposition. In the derivation process, we improve upon the best known constructions for block deletion-correcting codes (i.e., codes capable of correcting a block of consecutive deletions).

The paper is organized as follows. Section II contains the problem statement and relevant notation. Section III contains an analysis of the code design procedure for single deletion or single adjacent transposition correction. Section IV contains an order optimal code construction for correcting a single deletion and a single adjacent transposition, as well a low-redundancy construction for codes correcting a single deletion and multiple adjacent transpositions. Sections V and VI are devoted to our main findings: The best known code construction for sin-

gle block deletion correction, and codes capable of correcting a single block deletion and a single adjacent block transposition.

II. TERMINOLOGY AND NOTATION

We start by defining the *Damerau-Levenshtein distance*, which arose in the works of Damerau [8] and Levenshtein [15], and by introducing codes in this metric. We then proceed to extend the underlying coding problem so that it applies to blocks, rather than individual symbol errors.

Definition 1. The *Damerau-Levenshtein distance* is a string metric, which for two strings of possibly different lengths over some (finite) alphabet equals the minimum number of insertions, deletions, substitutions and adjacent transposition edits needed to transform one string into the other. The **block Damerau-Levenshtein distance** with block length b is a string metric, which for two strings of possibly different lengths over some (finite) alphabet equals the minimum number of insertions, deletions, substitutions and adjacent transposition edits of blocks of length at most b needed to transform one string into the other.

For simplicity, we focus on edits involving deletions and adjacent transpositions only, and with slight abuse of terminology refer to the underlying sequence comparison function as the Damerau metric¹. Furthermore, we restrict our attention to binary alphabets only. Generalizations to larger alphabet sizes may potentially be accomplished by a careful use of Tenengoltz up-down encoding, described in [1], [16], but this problem will be discussed elsewhere.

For a vector $\mathbf{x} \in \mathbb{F}_2^n$, let $\mathcal{B}_{TVD}(\mathbf{x})$ denote the set of vectors that may be obtained from \mathbf{x} by either at most one single adjacent transposition (T) or at most one single deletion (D). Note that the size of $\mathcal{B}_{TVD}(\mathbf{x})$ is $2r(\mathbf{x})$, where $r(\mathbf{x})$ is the number of runs in \mathbf{x} , i.e., the smallest number of nonoverlapping substrings involving the same symbol that “covers” the sequence.

Example 1. Suppose that $\mathbf{x} = (0, 0, 1, 1, 0) \in \mathbb{F}_2^5$. Then,

$$\mathcal{B}_{TVD}(\mathbf{x}) = \{(0, 1, 1, 0), (0, 0, 1, 0), (0, 0, 1, 1), (0, 0, 1, 1, 0), (0, 1, 0, 1, 0), (0, 0, 1, 0, 1)\}.$$

In particular, $\mathcal{B}_{TVD}(\mathbf{x}) = \mathcal{B}_D(\mathbf{x}) \cup \mathcal{B}_T(\mathbf{x})$, where $\mathcal{B}_D(\mathbf{x})$ is the set of words obtained by deleting at most one element in \mathbf{x} , while $\mathcal{B}_T(\mathbf{x})$ is the set of words obtained from at most one adjacent transposition in \mathbf{x} .

The derivative of \mathbf{x} , denoted by $\partial(\mathbf{x}) = \mathbf{x}'$ is a vector defined as $\mathbf{x}' = (x_1, x_2 + x_1, x_3 + x_2, \dots, x_n + x_{n-1})$. Clearly, the mapping between \mathbf{x} and \mathbf{x}' is a bijection. Hence, the integral $\partial^{-1}(\mathbf{x}) \triangleq \bar{\mathbf{x}}$ is well-defined for all $\mathbf{x} \in \mathbb{F}_2^n$. For a set $\mathcal{X} \subseteq \mathbb{F}_2^n$, we use \mathcal{X}' to denote the set of derivatives of vectors in \mathcal{X} , and similarly, we use $\bar{\mathcal{X}}$ to denote the set of integrals of vectors in \mathcal{X} . For two vectors $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$, we let $d_H(\mathbf{x}, \mathbf{y})$ denote their Hamming distance. Furthermore, we let $\mathcal{C}_H(n, d)$ stand for any code of length n with minimum Hamming distance d , and similarly, we let $\mathcal{C}_D(n)$ stand for any single-deletion-correcting code of length n .

¹Since we only consider deletions, what we refer to as Damerau distance is strictly speaking not a metric.

Similar notation will be used for other types of editing errors, balls, distances and codes, with their meaning apparent from the context. Furthermore, for the convenience of the reader, relevant notation and terminology referred to throughout the paper is summarized in Table I.

III. SINGLE TRANSPOSITION OR DELETION-CORRECTING CODES

We start by describing a general construction for single transposition or deletion-correcting codes. We then show how to use this construction in order to devise codes with near-optimal redundancy.

Construction 1 Let $\mathcal{C}_H(n, 3)$ be a single-error-correcting code, and, as before, let $\mathcal{C}_D(n)$ be a single-deletion-correcting code. We define a code $\mathcal{C}_{TVD}(n)$, which we show in Lemma 2 is capable of correcting one transposition (T) or (V) one deletion (D) as follows:

$$\mathcal{C}_{TVD}(n) = \{\mathbf{x} \in \mathbb{F}_2^n : \mathbf{x} \in \mathcal{C}_D(n), \bar{\mathbf{x}} \in \mathcal{C}_H(n, 3)\}.$$

Note that the code $\mathcal{C}_{TVD}(n)$ consists of codewords that belong to a single deletion error-correcting code and have integrals that belong to a single substitution error-correcting code.

Lemma 2. The code $\mathcal{C}_{TVD}(n)$ from Construction 1 can correct a single adjacent transposition or a single deletion.

Proof: We prove this claim by showing that for all $\mathbf{x} \in \mathcal{C}_{TVD}(n)$, one can uniquely recover \mathbf{x} from any $\mathbf{z} \in \mathcal{B}_{TVD}(\mathbf{x})$.

Assume first that $\mathbf{z} \in \mathbb{F}_2^{n-1}$, so that \mathbf{z} is the result of a single deletion occurring in \mathbf{x} . Since $\mathbf{x} \in \mathcal{C}_D(n)$, one may apply the decoder of the code $\mathcal{C}_D(n)$ to successfully recover $\mathbf{x} \in \mathcal{C}_{TVD}(n)$.

Assume that $\mathbf{z} \in \mathbb{F}_2^n$, so that \mathbf{z} is the result of at most one single transposition in \mathbf{x} . We show that $d_H(\bar{\mathbf{x}}, \bar{\mathbf{z}}) \leq 1$. When this inequality holds, since $\bar{\mathbf{x}}$ belongs to a code with minimum Hamming distance 3, the vector $\bar{\mathbf{x}}$ can be uniquely determined based on $\bar{\mathbf{z}}$. Note that since the mapping ∂ is injective, $d_H(\bar{\mathbf{x}}, \bar{\mathbf{z}}) = 0$ if and only if $\mathbf{x} = \mathbf{z}$.

Let the transmitted word \mathbf{x} be subjected to one adjacent transposition involving the i th and $(i+1)$ th bits, so that $x_i \neq x_{i+1}$ and $\mathbf{z} = (x_1, \dots, x_{i-1}, x_{i+1}, x_i, x_{i+2}, \dots, x_n)$. First, we compute the integral $\bar{\mathbf{z}}$ as

$$\bar{\mathbf{z}} = (z_1, z_2 + z_1, z_3 + z_2 + z_1, \dots, \sum_{j=1}^n z_j) = (\bar{z}_1, \dots, \bar{z}_n).$$

Let $\bar{\mathbf{x}} = (\bar{x}_1, \dots, \bar{x}_n)$. Then, clearly $(\bar{x}_1, \dots, \bar{x}_{i-1}) = (\bar{z}_1, \dots, \bar{z}_{i-1})$. Furthermore,

$$\bar{z}_i = \sum_{j=1}^{i-1} x_j + x_{i+1} = \sum_{j=1}^{i-1} x_j + (1 + x_i) = 1 + \bar{x}_i,$$

and for any $k \geq i+1$, $\bar{z}_k = \sum_{j=1}^{i-1} x_j + x_{i+1} + x_i + \sum_{j=i+2}^k x_j = \bar{x}_k$, so that $d_H(\bar{\mathbf{x}}, \bar{\mathbf{z}}) = 1$ as desired. ■

Note that we did not explicitly state in Construction 1 which codes to use. An obvious choice would be a Hamming code as the single substitution error-correcting code and the Varshamov-Tenengoltz (VT) code as the single deletion error-correcting

Notation	Description	Position in the manuscript
$\mathcal{B}_D(\mathbf{x})$	The set of words that may be obtained from at most one single deletion in a vector \mathbf{x} .	End of Section II.
$\mathcal{B}_T(\mathbf{x})$	The set of words that may be obtained from at most one single adjacent transposition in a vector \mathbf{x} .	End of Section II.
$\mathcal{B}_{T \vee D}(\mathbf{x})$	$\mathcal{B}_{T \vee D}(\mathbf{x}) = \mathcal{B}_D(\mathbf{x}) \cup \mathcal{B}_T(\mathbf{x})$.	End of Section II.
$\mathbf{x}', \partial(\mathbf{x})$	The derivative of \mathbf{x} .	End of Section II.
$\bar{\mathbf{x}}, \partial^{-1}(\mathbf{x})$	The integral of \mathbf{x}	End of Section II.
$\mathcal{C}_H(n, d)$	A code of minimum Hamming distance d .	End of Section II.
$\mathcal{C}_{T \vee D}(n)$	A code that can correct a single adjacent transposition or deletion.	Section III, Construction 1.
$\mathbf{X}_D(n, a)$	A code that can correct a single deletion error.	Section III, preceding Claim 1.
$\mathbf{X}_H(n, a)$	A code that can correct a single substitution error.	Section III, preceding Claim 1.
$\mathcal{B}_{(T, \ell)}(\mathbf{x})$	The set of words obtained from \mathbf{x} via ℓ adjacent transpositions.	Section IV, preceding Example 2.
$\mathcal{B}_{(T, \ell), D}(\mathbf{x})$	The set of words obtained from \mathbf{x} via ℓ adjacent transpositions and a single deletion.	Section IV, preceding Example 2.
$\mathcal{C}_{VT}(n, a, \ell)$	A VT-type code taken with modulus given by the parameter ℓ . The code $\mathcal{C}_{VT}(n, a, b, \ell)$ comprises a subset of codewords in $\mathcal{C}_{VT}(n, a, \ell)$ dictated by the parameter b .	Section IV, following Lemma 6.
$\mathcal{D}_{VT, n, \ell}$	A decoder for $\mathcal{C}_{VT}(n, a, \ell)$.	Section IV, following Lemma 6.
$\mathcal{D}_{VT, n, b, \ell}$	A decoder for $\mathcal{C}_{VT}(n, a, b, \ell)$.	Section IV, following Lemma 8.
$\mathcal{C}_{(T, \ell) \wedge D}(n, a, b)$	A code which may correct a single deletion and up to ℓ adjacent transpositions. $\mathcal{C}_{(T, \ell) \wedge D}(n, a, b)$ is a subset of words in $\mathcal{C}_{VT}(n, a, b, \ell)$.	Section IV, before Theorem 11.
$\mathbf{Y}_{T \wedge D}(n, a_1, a_2)$	A code used in the definition of $\mathcal{C}_{T \wedge D}(n, a_1, a_2)$.	Section IV, following Corollary 12.
$\mathcal{C}_{T \wedge D}(n, a_1, a_2)$	A code that may correct one adjacent transposition and one deletion.	Section IV, following Corollary 12.
$\mathcal{B}_{D, \leq b}(\mathbf{x})$	The set of words that may be obtained from \mathbf{x} via a burst of consecutive deletions of length at most b .	Section V-A, Part 1.
$\mathcal{B}_{D, b}(\mathbf{x})$	The set of words that may be obtained from \mathbf{x} via a burst of consecutive deletions of length exactly b .	Section V-A, Part 1.
$\mathcal{C}_{par}(n, b, \mathbf{d})$	A code used to determine the weight of a deleted substring.	Section V-A, Part 1.
$I(\mathbf{y}, \mathbf{v}, k_I)$	A vector obtained by inserting \mathbf{v} into \mathbf{y} at position k_I .	Section V-A, preceding Claim 3.
$D(\mathbf{y}, b, k_D)$	A vector obtained by deleting b consecutive bits from \mathbf{y} starting at position k_D .	Section V-A, preceding Claim 3.
$Bal(n, b)$	A (balanced) set of words in which any sufficiently long substring has roughly half ones and half zeros.	Section V-A, preceding Claim 4.
$\mathcal{C}_b^{odd}(n, a, \mathbf{D})$	A code for determining the approximate location of a burst of deletions. The code $\mathcal{C}_{VT}(n, a, b, \ell)$ comprises a subset of words in $\mathcal{C}_{VT}(n, a, \ell)$.	Section V-A, following Claim 4.
$SVT_{c, d}(n, M)$	A code for determining the exact location of a deletion given an approximate location for the same.	Section V-A, Part 3.
$\mathcal{C}_b^{odd}(n, a, \mathbf{C}, \mathbf{D})$	A code which may correct a burst of deletions of odd length. The code $\mathcal{C}_b^{odd}(n, a, \mathbf{C}, \mathbf{D})$ is constructed using the codes $\mathcal{C}_b^{odd}(n, a, \mathbf{D})$ and $SVT_{c, d}(n, M)$.	Section V-A, preceding Theorem 17.
$\mathcal{C}_b(n, a, \bar{\mathbf{C}}, \bar{\mathbf{D}})$	A code capable of correcting a burst of deletions of any length $\leq b$. $\mathcal{C}_b(n, a, \bar{\mathbf{C}}, \bar{\mathbf{D}})$ is constructed using the code $\mathcal{C}_b^{odd}(n, a, \mathbf{C}, \mathbf{D})$.	Section V-B, following Example 9.
$\mathcal{B}_{BT, b}(\mathbf{x})$	The set of words obtained from \mathbf{x} via one adjacent block transposition.	Section VI, preceding Example 11.
$\mathcal{B}_{BT \wedge D, b}(\mathbf{x})$	The set of words obtained from \mathbf{x} via one adjacent block transposition and one block deletion.	Section VI, following Example 12.
$T(\mathbf{x}, k_T)$	The vector resulting from transposing the symbols at positions k_T and $k_T + 1$ in \mathbf{x} .	Section VI, preceding Lemma 22.
$\mathcal{C}_{TD, b}^{(1)}(n, a, \mathbf{C}, \mathbf{D})$	A code for determining the approximate location of a block of deletions and adjacent transposition.	Section VI, following Lemma 22.
$\mathcal{C}(n, m; t_1, t_2)$	A code for correcting special types of burst errors.	Section VI, following Definition 24.
$\mathcal{C}_b^{Odd, B}(n, a, \mathbf{C}, \mathbf{D})$	A code for correcting an odd-length block of deletions and adjacent block transposition.	Section VI, following Lemma 22.
$\mathcal{C}_{TD, b}(n, a, \bar{\mathbf{C}}, \bar{\mathbf{D}})$	A code for correcting one block of deletions and one adjacent block transposition.	Section VI, before Theorem 27.

TABLE I
RELEVANT NOTATION AND TERMINOLOGY.

code [15], or any coset of these codes. Since the cosets of these codes cover \mathbb{F}_2^n , one can see that there exists a code with redundancy at most $2 \log(n+1)$. We show next how to improve this result by constructing one code that can serve both as a single deletion-correcting for \mathbf{x} and a single error-correcting code for $\bar{\mathbf{x}}$. The redundancy of this code is at most $\log n + \log 6$.

Our choice of codes is as follows. Let a be a non-negative integer such that $0 \leq a \leq 6n - 4$. For the single deletion code,

$$\mathbf{X}_D(n, a) = \{\mathbf{x} \in \mathbb{F}_2^n : \sum_{i=1}^{n-1} i x_i + (2n-1)x_n \equiv a \pmod{(6n-3)}\}.$$

For the code $\mathcal{C}_H(n, 3)$, we choose

$$\mathbf{X}_H(n, a) = \left\{ \mathbf{x} \in \mathbb{F}_2^n : \sum_{i=1}^{n-2} (2i+1)x_i + (2(n-1)+1)x_n + (3(n-1)+1)x_{n-1} \equiv a \pmod{6n-3} \right\}.$$

Claim 1. For any vector $\mathbf{x} \in \mathbb{F}_2^n$, if $\mathbf{x}' \in \mathbf{X}_D(n, a)$ then $\mathbf{x} \in \mathbf{X}_H(n, a)$ and thus if $\mathbf{x} \in \mathbf{X}_D(n, a)$ then $\overline{\mathbf{x}} \in \mathbf{X}_H(n, a)$.

Proof: Suppose that $\mathbf{x}' \in \mathbf{X}_D(n, a)$. By definition,

$$\sum_{i=1}^{n-1} i x'_i + (2n-1)x'_n \equiv a \pmod{6n-3}.$$

Therefore, since $\mathbf{x}' = (x_1, x_1 + x_2, x_2 + x_3, \dots, x_{n-1} + x_n)$, we have

$$x_1 + \sum_{i=2}^{n-1} i(x_i + x_{i-1}) + (2n-1)(x_{n-1} + x_n) \equiv a \pmod{6n-3},$$

which implies that $\mathbf{x} \in \mathbf{X}_H(n, a)$. This proves the claim. ■

According to Claim 1 and Lemma 2, in order to show that the code $\mathcal{C}_{T \vee D}(n) = \mathbf{X}_D(n, a)$ is a single transposition or deletion-correcting code, we only have to show that the codes $\mathbf{X}_D(n, a)$ and $\mathbf{X}_H(n, a)$ have the desired error-correcting properties.

Lemma 3. The code $\mathbf{X}_H(n, a)$ is a single substitution error-correcting code.

Proof: Let $H = (3, 5, 7, \dots, 2n-3, 3n-2, 2n-1)$ so that $\mathbf{x} \in \mathbf{X}_H(n, a)$ if and only if $H \mathbf{x}^T \equiv a \pmod{6n-3}$. Assume on the contrary that $\mathbf{X}_H(n, a)$ is not a single substitution error-correcting code. Then, there exist two different code-words $\mathbf{x}_1, \mathbf{x}_2 \in \mathbf{X}_H(n, a)$ and two vectors $\mathbf{e}_j, \mathbf{e}_k$ such that $\mathbf{x}_1 + \mathbf{e}_j = \mathbf{x}_1 + \mathbf{e}_k$, where both $\mathbf{e}_j, \mathbf{e}_k$ have at most a single non-zero entry of value 1 or -1 . Hence, we would have

$$H(\mathbf{x}_1 + \mathbf{e}_j)^T \equiv H(\mathbf{x}_2 + \mathbf{e}_k)^T \pmod{6n-3}, \text{ and } H \mathbf{e}_j^T \not\equiv H \mathbf{e}_k^T \pmod{6n-3},$$

which holds if and only if $\mathbf{e}_j = \mathbf{e}_k$. Therefore, we must have that $\mathbf{x}_1 = \mathbf{x}_2$, a contradiction. ■

Lemma 4. The code $\mathbf{X}_D(n, a)$ can correct a single deletion.

Proof: By definition, if $\mathbf{x} \in \mathbf{X}_D(n, a)$, we may write

$$H \mathbf{x}^T \equiv a \pmod{6n-3},$$

where $H = (1, 2, 3, \dots, n-1, 2n-1)$. The result follows by observing that $(1, 2, 3, \dots, n-1, 2n-1)$ is a Helberg sequence as defined in Definition III.2 from [11]. Thus, according to Theorem III.4 of the same paper, the code $\mathbf{X}_D(n, a)$ can correct a single deletion. ■

The following corollary summarizes the main result of this section.

Corollary 5. There exists a single transposition or deletion-correcting code whose redundancy is at most $\log(6n-3)$ bits.

Proof: Using the pigeon-hole principle considered in [21], one may easily show that $|\mathbf{X}_H(n, a)| = |\mathcal{C}_{T \vee D}(n, a)| \geq \frac{2^n}{6n-3}$, since $\mathcal{C}_{T \vee D}(a, n)$ partitions the ambient space \mathbb{F}_2^n into $6n-3$ codes, one of which has to have a size at least as large as the right-hand side of the inequality. ■

Note that every single transposition or deletion-correcting code is also a single deletion error-correcting code. Hence, a lower bound on the redundancy of the latter code is $\log n$ [13], so that the difference between the redundancy of our deletion/adjacent transposition codes and the redundancy of a optimal single deletion code is at most $\log 6$ bits. We also note that improving the lower bound on a single transposition or deletion-correcting code is left as an open problem.

IV. CODES CORRECTING DELETIONS AND ADJACENT TRANSPOSITIONS

We now turn our attention to the significantly more challenging task of constructing codes that can correct both deletions and adjacent transpositions simultaneously. Our main result is a construction of a code capable of correcting a single deletion along with multiple adjacent transpositions. At the end of this section, we present an improved construction for the special case of a single deletion and a single transposition.

We start by introducing some useful notation. Let $\mathcal{B}_{(T, \ell)}(\mathbf{x})$ denote the set of vectors that may be obtained by applying at most ℓ adjacent transpositions (T) to \mathbf{x} . Hence,

$$\mathcal{B}_{(T, \ell)}(\mathbf{x}) = \underbrace{\mathcal{B}_{(T, 1)}(\dots(\mathcal{B}_{(T, 1)}(\mathbf{x}))\dots)}_{\ell \text{ times}}.$$

Let $\mathcal{B}_{(T, \ell), D}(\mathbf{x})$ denote the set of vectors that may be obtained from \mathbf{x} by at most ℓ adjacent transpositions followed by at most one single deletion. As before, let $\mathcal{B}_D(\mathbf{x})$ be the set of words that may be obtained by introducing at most one deletion into \mathbf{x} . With a slight abuse of notation, we use the same symbol \mathcal{B} independently on the the argument of the set being a word or a collection of words. In the latter case, the set \mathcal{B} equals the union of the corresponding sets of individual words in the argument. The next example illustrates the relevant notation.

Example 2. Suppose that $\mathbf{x} = (0, 0, 1, 1, 0)$. Then,

$$\mathcal{B}_{(T, 1)}(\mathbf{x}) = \{(0, 0, 1, 1, 0), (0, 1, 0, 1, 0), (0, 0, 1, 0, 1)\},$$

$$\mathcal{B}_D(\mathbf{x}) = \{(0, 0, 1, 1, 0), (0, 1, 1, 0), (0, 0, 1, 0), (0, 0, 1, 1)\},$$

$$\mathcal{B}_{(T, 1), D}(\mathbf{x}) = \{(0, 0, 1, 1, 0), (0, 1, 1, 0), (0, 0, 1, 0), (0, 0, 1, 1), (1, 0, 1, 0), (0, 1, 0, 1), (0, 1, 0, 0), (0, 0, 0, 1)\}.$$

Lemma 6. For any $\mathbf{x} \in \mathbb{F}_2^n$,

$$\mathcal{B}_{(T, \ell), D}(\mathbf{x}) = \mathcal{B}_D(\mathcal{B}_{(T, \ell)}(\mathbf{x})) = \mathcal{B}_{(T, \ell)}(\mathcal{B}_D(\mathbf{x})).$$

Proof: The proof is by induction on ℓ . For the base case $\ell = 1$, we show that $\mathcal{B}_D(\mathcal{B}_{(T, 1)}(\mathbf{x})) = \mathcal{B}_{(T, 1)}(\mathcal{B}_D(\mathbf{x}))$ by demonstrating that if $\mathbf{y} \in \mathcal{B}_{(T, 1)}(\mathcal{B}_D(\mathbf{x}))$, then $\mathbf{y} \in \mathcal{B}_D(\mathcal{B}_{(T, 1)}(\mathbf{x}))$. Furthermore if $\mathbf{y} \in \mathcal{B}_D(\mathcal{B}_{(T, 1)}(\mathbf{x}))$, then $\mathbf{y} \in \mathcal{B}_{(T, 1)}(\mathcal{B}_D(\mathbf{x}))$.

Suppose that $\mathbf{y}^{(d)} = (x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n)$ is the result of deleting the symbol at position i , where $i \in [n]$. Also, assume that $\mathbf{y} = \mathbf{y}^{(d,t)}$ is obtained from $\mathbf{y}^{(d)}$ by transposing the symbol in position j with the symbol in position $j+1$ in $\mathbf{y}^{(d)}$, where $j \in [n-2]$. One needs to consider two different scenarios: 1) $j \in [n-2] \setminus (i-1)$; and 2) $j = i-1$.

First, we show that if $j \in [n-2] \setminus (i-1)$, then $\mathbf{y} \in \mathcal{B}_D(\mathcal{B}_{(T,1)}(\mathbf{x}))$. To see why this claim holds, note that if $j < i-1$ then \mathbf{y} may be generated by first transposing the symbols in positions $j, j+1$ in \mathbf{x} to obtain $\mathbf{y}^{(t)}$ and then deleting the symbol in position i . Otherwise, if $j \geq i$, one may first transpose the symbols in positions $j+1, j+2$, and then delete the symbol in position i . Suppose now that $j = i-1$. Then $x_{i-1} \neq x_{i+1}$ and so x_i equals either x_{i-1} or x_{i+1} . Suppose that $x_i = x_{i-1}$. Then \mathbf{y} may be generated by first transposing x_i and x_{i+1} , and then deleting the symbol in position $i-1$. Otherwise, if $x_i = x_{i+1}$, \mathbf{y} may be obtained by first transposing x_{i-1} and x_i and then deleting the symbol in position $i+1$.

Using a similar argument, it can be shown that if $\mathbf{y} \in \mathcal{B}_D(\mathcal{B}_{(T,1)}(\mathbf{x}))$, then $\mathbf{y} \in \mathcal{B}_{(T,1)}(\mathcal{B}_D(\mathbf{x}))$. This establishes the base case $\mathcal{B}_D(\mathcal{B}_{(T,1)}(\mathbf{x})) = \mathcal{B}_{(T,1)}(\mathcal{B}_D(\mathbf{x}))$.

We now prove the inductive step.

Suppose that $\mathcal{B}_D(\mathcal{B}_{(T,\ell)}(\mathbf{x})) = \mathcal{B}_{(T,\ell)}(\mathcal{B}_D(\mathbf{x}))$ holds for all $\ell < L$. We show that $\mathcal{B}_D(\mathcal{B}_{(T,L)}(\mathbf{x})) = \mathcal{B}_{(T,L)}(\mathcal{B}_D(\mathbf{x}))$ holds as well. This may be seen from the following chain of equalities:

$$\begin{aligned} \mathcal{B}_D(\mathcal{B}_{(T,L)}(\mathbf{x})) &= \mathcal{B}_D(\mathcal{B}_{(T,L-1)}(\mathcal{B}_{(T,1)}(\mathbf{x}))) \\ &= \mathcal{B}_{(T,L-1)}(\mathcal{B}_D(\mathcal{B}_{(T,1)}(\mathbf{x}))) \\ &= \mathcal{B}_{(T,L-1)}(\mathcal{B}_{(T,1)}(\mathcal{B}_D(\mathbf{x}))) \\ &= \mathcal{B}_{(T,L)}(\mathcal{B}_D(\mathbf{x})), \end{aligned}$$

where the second line follows from the inductive hypothesis, which is applied to each vector in the set, and where the third line is a result of the previous result which showed that $\mathcal{B}_D(\mathcal{B}_{(T,1)}(\mathbf{x})) = \mathcal{B}_{(T,1)}(\mathcal{B}_D(\mathbf{x}))$. ■

As a consequence of the previous lemma, we may henceforth assume that the deletion always occurs after the adjacent transposition(s). We then say that a code \mathcal{C} can correct ℓ adjacent transpositions and a single deletion, and refer to it as a ℓ -TD code if for any two different codewords $\mathbf{u}, \mathbf{v} \in \mathcal{C}$, $\mathcal{B}_{(T,\ell),D}(\mathbf{u}) \cap \mathcal{B}_{(T,\ell),D}(\mathbf{v}) = \emptyset$. Our code construction and the ideas behind the coding approach are best explained through the decoding procedure.

Suppose that the code $\mathcal{C}_{T \wedge D}(n, \ell)$ is an ℓ -TD code, which is a subset of codewords of a single deletion-correcting code. Assume also that $\mathbf{x} \in \mathcal{C}_{T \wedge D}(n, \ell)$ was transmitted and that the vector \mathbf{y} was received, where \mathbf{y} is the result of at most ℓ transpositions followed by at most one single deletion in \mathbf{x} . The simplest idea to pursue is to try to correct the single deletion by naively applying the decoder for the chosen constituent single-deletion code. Clearly, such a decoder may produce an erroneous result due to the presence of the adjacent transposition errors. It is therefore important to construct the code $\mathcal{C}_{T \wedge D}(n, \ell)$ in such a way that the result of the “mismatched” deletion correction $\hat{\mathbf{x}}$, obtained from \mathbf{y} , is easy to characterize and contains only a limited number of errors that may be corrected to recover

$\mathbf{x} \in \mathcal{C}_{T \wedge D}(n, \ell)$ from $\hat{\mathbf{x}}$. To this end, define the following code:

$$\mathcal{C}_{VT}(n, a, \ell) = \{\mathbf{x} \in \mathbb{F}_2^n : \sum_{i=1}^n i x_i \equiv a \pmod{n+2\ell+1}\}.$$

Since the code is a VT code, the decoder $\mathcal{D}_{VT,n,\ell}$ for $\mathcal{C}_{VT}(n, a, \ell)$ can correct a single deletion occurring in any codeword in $\mathcal{C}_{VT}(n, a, \ell)$ [21]. Note that the standard definition of a single deletion-correcting code entails setting $\sum_{i=1}^n i x_i$ to be equal to some a modulo $n+1$ [21]. Our construction fixes $\sum_{i=1}^n i x_i$ to a modulo $n+2\ell+1$ instead. As we demonstrate in Claim 2, this change is needed due to the fact that adjacent transpositions may change the value of the syndrome a by at most $\pm \ell$.

As before, and for the special case of VT codes, assume that $\hat{\mathbf{x}}$ is the result of VT decoding the vector \mathbf{y} where $\mathbf{y} \in \mathcal{B}_{(T,\ell),D}(\mathbf{x})$. Our first aim is to characterize the difference between $\hat{\mathbf{x}}$ and \mathbf{x} , and for this purpose we use an intermediary word $\mathbf{y}^{(\ell)}$ that is generated from at most ℓ adjacent transpositions in \mathbf{x} , i.e., a word such that $\mathbf{y} \in \mathcal{B}_D(\mathbf{y}^{(\ell)})$. More precisely, we demonstrate that if both $\mathbf{x}, \mathbf{y}^{(\ell)} \in \mathcal{C}_{VT}(n, a, \ell)$, then the decoder outputs $\mathcal{D}_{VT,n,\ell}(a, \mathbf{y})$ and $\mathcal{D}_{VT,n,\ell}(a, \mathbf{y}^{(\ell)})$ will differ only in the transpositions that actually occurred in \mathbf{x} . On the other hand, if $\mathbf{x}, \mathbf{y}^{(\ell)}$ belong to two different VT codes (i.e. they have different values of the VT syndrome parameter a), then \mathbf{x} and $\hat{\mathbf{x}}$ differ by at most 2ℓ adjacent transpositions. The following simple claim is a consequence of the fact that an adjacent transposition changes the VT syndrome by at most one.

Claim 2. Suppose that $\mathbf{y}^{(\ell)} = (y_1^{(\ell)}, \dots, y_n^{(\ell)}) \in \mathcal{B}_{(T,\ell)}(\mathbf{x})$ where $\mathbf{x} \in \mathbb{F}_2^n$. Then, one has $|\sum_{i=1}^n i x_i - \sum_{i=1}^n i y_i^{(\ell)}| \leq \ell$.

Proof: The proof is by induction on ℓ . For the base case suppose $\mathbf{y}^{(1)} \in \mathcal{B}_{(T,1)}(\mathbf{x})$. The result clearly holds if $\mathbf{y}^{(1)} = \mathbf{x}$ and so assume $\mathbf{y}^{(1)}$ is the result of transposing the symbols in positions j and $j+1$ in \mathbf{x} . Then

$$\begin{aligned} & \left| \sum_{i=1}^n i x_i - \sum_{i=1}^n i y_i^{(1)} \right| \\ &= \left| i x_i + (i+1) x_{i+1} - (i x_{i+1} + (i+1) x_i) \right| \\ &= |x_{i+1} - x_i| = 1, \end{aligned}$$

since $x_i \neq x_{i+1}$. For the inductive step, suppose that the result holds for all $\ell < L$ and consider the case $\ell = L$. Let $\mathbf{y}^{(L)} \in \mathcal{B}_{(T,L)}$ and let $\mathbf{y}^{(L-1)} \in \mathcal{B}_{(T,L-1)}$ be such that $\mathbf{y}^{(L)}$ and $\mathbf{y}^{(L-1)}$ differ by at most one single adjacent transposition. Then,

$$\begin{aligned} & \left| \sum_{i=1}^n i x_i - \sum_{i=1}^n i y_i^{(L)} \right| \\ &= \left| \sum_{i=1}^n i x_i - \sum_{i=1}^n i y_i^{(L-1)} + \sum_{i=1}^n i y_i^{(L-1)} - \sum_{i=1}^n i y_i^{(L)} \right| \\ &\leq \left| \sum_{i=1}^n i x_i - \sum_{i=1}^n i y_i^{(L-1)} \right| + \left| \sum_{i=1}^n i y_i^{(L-1)} - \sum_{i=1}^n i y_i^{(L)} \right| \\ &\leq L-1 + 1 = L. \end{aligned}$$

■

As a consequence of the previous claim, if $\mathbf{x} \in \mathcal{C}_{VT}(n, a, \ell)$ and $\mathbf{y}^{(\ell)} \in \mathcal{B}_{(T,\ell)}(\mathbf{x})$, then $\mathbf{y}^{(\ell)} \in \mathcal{C}_{VT}(n, \hat{a}, \ell)$ for some \hat{a} ,

where $|a - \hat{a}| \leq \ell$. The next lemma summarizes the previous discussion.

Lemma 7. Suppose that $\mathbf{y}^{(\ell)} \in \mathcal{B}_{(T,\ell)}(\mathbf{x})$, where $\mathbf{x} \in \mathcal{C}_{VT}(n, a, \ell)$, and let $\mathbf{y} \in \mathcal{B}_D(\mathbf{y}^{(\ell)})$. Then, $\mathcal{D}_{VT,n,\ell}(\hat{a}, \mathbf{y}) = \mathbf{y}^{(\ell)}$ for some \hat{a} such that $|a - \hat{a}| \leq \ell$.

Example 3. Suppose that $\mathbf{x} = (0, 1, 1, 0, 0, 1, 0, \mathbf{0}, 0, 0, 1, 0) \in \mathcal{C}_{VT}(12, 3, 3)$ was transmitted and that the vector $\mathbf{y} = (0, 1, 1, 0, 0, 1, 0, \mathbf{0}, 1, 0, \mathbf{0}, 0)$ was received after at most three adjacent transpositions and a single deletion. For $\mathbf{y}^{(3)} = (0, 1, 1, 0, 0, 1, 0, \mathbf{0}, 0, \mathbf{1}, \mathbf{0}, 0)$ (where $\mathbf{y} \in \mathcal{B}_D(\mathbf{y}^{(3)})$), we have $\sum_{i=1}^{n-1} y_i \equiv 2 \pmod{19}$. Thus, since $a = 3$ and $\hat{a} = 2$, we get that $|a - \hat{a}| \leq 1 \leq \ell = 3$ as desired.

Note that if we use the decoder $\mathcal{D}_{VT,12,3}$ we arrive at $\hat{\mathbf{x}} = \mathcal{D}_{VT,12,3}(\mathbf{3}, \mathbf{y}) = (0, 1, 1, 0, 0, \mathbf{0}, 1, 0, 0, \mathbf{1}, \mathbf{0}, 0)$. Hence, we have $\hat{\mathbf{x}} = (0, 1, 1, 0, 0, \mathbf{0}, 1, 0, 0, \mathbf{1}, \mathbf{0}, 0)$, and $\mathbf{x} = (0, 1, 1, 0, 0, 1, 0, \mathbf{0}, 0, 0, 1, 0)$.

We characterize next the difference between $\mathcal{D}_{VT,n,\ell}(a, \mathbf{y})$ and $\mathcal{D}_{VT,n,\ell}(\hat{a}, \mathbf{y})$ for the case that $|a - \hat{a}| \leq \ell$, as the value \hat{a} is not known beforehand. Our main result may be intuitively described as follows: Suppose that $\mathbf{y} \in \mathcal{B}_D(\mathbf{x})$, where $\mathbf{x} \in \mathcal{C}_{VT}(n, a, \ell)$ and where \mathbf{y} is obtained by deleting the k th bit, x_k , from \mathbf{x} . Also, assume that the value of x_k is known to the decoder and that $\hat{\mathbf{x}} = \mathcal{D}_{VT,n,\ell}(a + v, \mathbf{y})$, for some offset v , is obtained by inserting the bit x_k into \mathbf{y} at some position determined by the decoder. Then, if $x_k = 0$, we may obtain \mathbf{x} from $\hat{\mathbf{x}}$ by sliding the inserted bit to the left/right using a series of adjacent transposition operations past at most v ones. Otherwise, if $x_k = 1$, then we can obtain \mathbf{x} from $\hat{\mathbf{x}}$ by sliding the inserted bit to the left/right past at most v zeros. The next lemma rigorously summarizes this observation.

Lemma 8. Suppose that \mathbf{y} is the result of a single deletion occurring in $\mathbf{x} \in \mathcal{C}_{VT}(n, a, \ell)$ at position k . Given k , let $v_L = |\{j \in [n] : j < k, x_j = 1\}|$ and $v_R = |\{j \in [n] : j > k, x_j = 1\}|$. Then,

- 1) If $x_k = 0$, then for all $v \in \{-v_R, -v_R + 1, \dots, v_L\}$, one may obtain $\mathcal{D}_{VT,n,\ell}(a + v, \mathbf{y})$ by inserting the symbol 0 into \mathbf{y} immediately after the $(v_L - v)$ -th one.
- 2) If $x_k = 1$, then for all $v \in \{-(k - 1) + v_L, -k + v_L + 2, \dots, (n - k) - v_R\}$, one may obtain $\mathcal{D}_{VT,n,\ell}(a + v, \mathbf{y})$ by inserting the symbol 1 into \mathbf{y} immediately after the $(v + k - v_L - 1)$ -th zero.

Example 4. Suppose that $\mathbf{x} = (0, 1, 1, 0, \mathbf{0}, 1, 0, 0, 0, 0, 1, 0) \in \mathcal{C}_{VT}(12, 3, 3)$, and that $\hat{\mathbf{x}} = \mathcal{D}_{VT,n,\ell}(\mathbf{3}, \mathbf{y})$, was obtained by VT decoding $\mathbf{y} = (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$. For $v = 2$, one has $\mathcal{D}_{VT,n,\ell}(5, \mathbf{y}) = (\mathbf{0}, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$, whereas for $v = -1$, one has $\mathcal{D}_{VT,n,\ell}(2, \mathbf{y}) = (0, 1, 1, 0, 1, \mathbf{0}, 0, 0, 0, 0, 1, 0)$.

Next, suppose that $\mathbf{y} = (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) - \mathbf{y}$ is the result of deleting the third 1 at position $k = 6$ from $\mathbf{x} = (0, 1, 1, 0, 0, \mathbf{1}, 0, 0, 0, 0, 1, 0)$. In this case, choosing $v = 3$ gives $\mathcal{D}_{VT,n,\ell}(6, \mathbf{y}) = (0, 1, 1, 0, 0, 0, 0, 0, \mathbf{1}, 0, 1, 0)$, while $v = -2$ gives $\mathcal{D}_{VT,n,\ell}(1, \mathbf{y}) = (0, \mathbf{1}, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$.

Proof of Lemma 8: Suppose first that \mathbf{y} is the result of deleting a zero from $\mathbf{x} \in \mathcal{C}_{VT}(n, a, \ell)$. Let $a' \equiv a - \sum_{i=1}^{n-1} y_i \pmod{n+2\ell+1}$.

The decoder $\mathcal{D}_{VT,n,\ell}$ for $\mathcal{C}_{VT}(n, a, \ell)$ produces the vector $\hat{\mathbf{x}} \in \mathcal{C}_{VT}(n, a, \ell)$ by inserting a zero into the first position k' that has a' ones to the right of it. If $x_k = 0$, then clearly $a' = v_R$, and the decoder correctly outputs \mathbf{x} so that $\hat{\mathbf{x}} = \mathbf{x}$. If the decoder $\mathcal{D}_{VT,n,\ell}$ for $\mathcal{C}_{VT}(n, a + v, \ell)$ were applied to \mathbf{y} instead, one would have

$$a'' \equiv a + v - \sum_{i=1}^{n-1} y_i \pmod{n+2\ell+1} \equiv a' + v \pmod{n+2\ell+1}.$$

Hence, the decoder $\mathcal{D}_{VT,n,\ell}$ for $\mathcal{C}_{VT}(n, a + v, \ell)$ would insert a zero in the vector \mathbf{y} at the first position k'' that has $a' + v$ ones to the right of it. The claim follows by observing that the position that has $a' + v$ ones after it is in the same run as the position in \mathbf{y} with $(v_L - v)$ ones preceding it.

Suppose next that \mathbf{y} is the result of deleting a one from $\mathbf{x} \in \mathcal{C}_{VT}(n, a, \ell)$. Let $a' \equiv a - \sum_{i=1}^{n-1} y_i \pmod{n+2\ell+1}$. The decoder $\mathcal{D}_{VT,n,\ell}$ for $\mathcal{C}_{VT}(n, a, \ell)$ produces the vector $\hat{\mathbf{x}} \in \mathcal{C}_{VT}(n, a, \ell)$ by inserting a one into the first position k' that has $a' - k'$ ones to the right of it. If $x_k = 1$, then clearly $k' = k$ and the decoder correctly outputs \mathbf{x} , so that $\hat{\mathbf{x}} = \mathbf{x}$.

If the decoder $\mathcal{D}_{VT,n,\ell}$ for $\mathcal{C}_{VT}(n, a + v, \ell)$ were applied to \mathbf{y} instead, then one would have $a'' \equiv a' + v \pmod{n+2\ell+1}$ as before. The decoder $\mathcal{D}_{VT,n,\ell}$ for $\mathcal{C}_{VT}(n, a + v, \ell)$ would insert a one into the vector \mathbf{y} at the first position k'' that has $a' + v - k''$ ones to the right of it. This produces a vector $\hat{\mathbf{x}}$. Since the first position k'' in \mathbf{y} with $a' + v - k''$ ones to the right is the same as the first position in \mathbf{y} following $(v + k - v_L - 1)$ zeros, the claimed result also follows for $x_k = 1$. ■

The previous lemma motivates the introduction of a modification of VT codes, which will be used as a constituent component in a construction of codes capable of correcting a deletion and multiple adjacent transpositions. This modified code structure also leads to a straightforward decoding procedure of the underlying codes. The code may be defined as follows:

$$\mathcal{C}_{VT}(n, a, b, \ell) = \{\mathbf{x} \in \mathbb{F}_2^n : \quad (1)$$

$$\begin{aligned} \sum_{i=1}^n x_i &\equiv a \pmod{n+2\ell+1}, \\ \sum_{i=1}^n x_i &\equiv b \pmod{2}. \end{aligned}$$

The decoder for $\mathcal{C}_{VT}(n, a, b, \ell)$, denoted by $\mathcal{D}_{VT,n,b,\ell}$, operates as follows. Suppose that $\mathbf{x} \in \mathcal{C}_{VT}(n, a, b, \ell)$ is transmitted and that $\mathbf{y} \in \mathcal{B}_{(T,\ell),D}(\mathbf{x})$ is received. Suppose that n_1 denotes the number of ones in \mathbf{y} . Then, for $a \in \mathbb{Z}_{n+2\ell+1}$ and $b \in \mathbb{F}_2$, $\mathcal{D}_{VT,n,b,\ell}(a, \mathbf{y})$ executes the following steps:

- 1) Set $x \equiv \sum_{i=1}^{n-1} y_i + b \pmod{2}$.
- 2) Compute $a' \equiv a - \sum_{i=1}^{n-1} y_i \pmod{n+2\ell+1}$.
- 3) If $x = 0$ and $a' \in \{0, 1, \dots, n_1\}$, insert a zero into the first position in \mathbf{y} that has a' ones on its right. If $a' \in \{n_1 + 1, n_1 + 2, \dots, n_1 + \ell\}$, insert a zero in the first position in \mathbf{y} . If $a' \in \{n + \ell + 1, n + \ell + 2, \dots, n + 2\ell\}$, insert a zero in the last position of \mathbf{y} .

- 4) If $x = 1$ and $a' \in \{n_1 + 1, n_1 + 2, \dots, n\}$, insert a one in the first position k of \mathbf{y} that has $a' - k$ ones to its right. Otherwise, if $a' \in \{n + 1, n + 2, \dots, n + \ell\}$, insert a one in the last position of \mathbf{y} . If $a' \in \{n_1 - \ell + 1, n_1 - \ell + 2, \dots, n_1\}$, insert a one in the first position of \mathbf{y} .

Note that the VT decoder discussed so far aims to correct a single deletion only, but potentially in a mismatched fashion as additional adjacent transposition errors may have been incurred during deletion correction. The output of the deletion-correcting decoder has to be fed into the input of a transposition error-correcting code, and we describe how this subsequent decoding is accomplished after providing an illustration of the VT decoding process.

Example 5. Suppose that $\mathbf{x} = (0, 1, 1, 0, \mathbf{0}, 1, 0, 0, 0, 0, 1, 0) \in \mathcal{C}_{VT}(12, 3, 0, 3)$, and that $\mathbf{y} = (0, 1, 1, 0, 1, 0, 0, 0, \mathbf{1}, \mathbf{0}, 0)$ is the received word, which is the result of a single deletion and a single transposition. We first apply the decoder $\mathcal{D}_{VT,12,0,3}$ to \mathbf{y} . In the first step of the procedure, we conclude that the deleted bit has value $x = 0$. In the second step of decoding, we compute $a' = 3$. Since $0 \leq a' \leq 4$, we have $\hat{\mathbf{x}} = (0, 1, \mathbf{0}, 1, 0, 1, 0, 0, 0, \mathbf{1}, \mathbf{0}, 0)$. Note that $\hat{\mathbf{x}} = (0, 1, \mathbf{0}, \mathbf{1}, 0, 1, 0, 0, 0, \mathbf{1}, \mathbf{0}, 0)$, and $\mathbf{x} = (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$, differ in *two* adjacent transpositions.

The previous example illustrates that \mathbf{x} and $\hat{\mathbf{x}}$ differ in a limited number of transpositions which depends on the original number of transposition errors. In particular, for the given example, the two vectors differ in two adjacent transpositions as $\hat{\mathbf{x}}$ is the result of a single deletion and a single transposition in \mathbf{y} . The next lemma gives a more precise characterization of the “distance” between \mathbf{x} and $\hat{\mathbf{x}}$.

Lemma 9. Suppose that $\mathbf{y}^{(\ell)} \in \mathcal{B}_{(T,\ell)}(\mathbf{x})$ where $\mathbf{x} \in \mathcal{C}_{VT}(n, a, b, \ell)$ and where $\mathbf{y} \in \mathcal{B}_D(\mathbf{y}^{(\ell)})$. Let $\hat{\mathbf{x}} = \mathcal{D}_{VT,n,b,\ell}(a, \mathbf{y})$. Then the following statements are true:

- 1) If $\hat{\mathbf{x}}$ is the result of inserting a zero in \mathbf{y} in a position with v_R ones to the right of the inserted bit, then $\mathbf{y}^{(\ell)}$ can be obtained from \mathbf{y} by inserting a zero in the first position with j ones to the right of it where $j \in \{v_R - \ell, v_R - \ell + 1, \dots, v_R + \ell\}$.
- 2) If $\hat{\mathbf{x}}$ is the result of inserting a one in \mathbf{y} in position k with v_R ones to the right of the inserted bit, then $\mathbf{y}^{(\ell)}$ can be obtained from \mathbf{y} by inserting a one in \mathbf{y} in the first position j with j_1 ones to the right of it where $j + j_1 \in \{k + v_R - \ell, k + v_R - \ell + 1, \dots, k + v_R + \ell\}$.

The following corollary summarizes one of the main results of this section.

Corollary 10. Suppose that $\mathbf{y} \in \mathcal{B}_{(T,\ell),D}(\mathbf{x})$ where $\mathbf{x} \in \mathcal{C}_{VT}(n, a, b, \ell)$ and let $\hat{\mathbf{x}} = \mathcal{D}_{VT,n,b,\ell}(a, \mathbf{y})$. Then $\mathbf{x} \in \mathcal{B}_{(T,2\ell)}(\hat{\mathbf{x}})$.

Consequently, the mismatched VT decoder increases the number of adjacent transposition errors by at most a factor of two.

Based on the results on mismatched VT decoding and Corollary 10, we are now ready to define a family of codes capable of correcting a single deletion and multiple adjacent transposition errors. Recall that given a binary word \mathbf{x} , its derivative $\partial(\mathbf{x}) = \mathbf{x}'$ is defined as $\mathbf{x}' = (x_1, x_2 + x_1, x_3 + x_2, \dots, x_n + x_{n-1})$ and its inverse as $\partial^{-1}(\mathbf{x}) = \bar{\mathbf{x}} = (x_1, x_1 + x_2, \dots, \sum_{i=1}^n x_i)$. We claim that the code $\mathcal{C}_{(T,\ell)\wedge D} \subseteq \mathbb{F}_2^n$, defined as

$$\mathcal{C}_{(T,\ell)\wedge D}(n, a, b) = \{\mathbf{x} \in \mathbb{F}_2^n : \bar{\mathbf{x}} \in \mathcal{C}_H(n, 4\ell + 1), \mathbf{x} \in \mathcal{C}_{VT}(n, a, b, \ell)\} \quad (2)$$

is an ℓ -TD code (i.e., a code capable of correcting ℓ adjacent transpositions (T, ℓ) and (\wedge) one deletion (D)).

Theorem 11. The code $\mathcal{C}_{(T,\ell)\wedge D}(n, a, b)$ is an ℓ -TD code.

Proof: Suppose that $\mathbf{y} \in \mathcal{B}_{(T,\ell),D}(\mathbf{x})$. We show how to recover \mathbf{x} from \mathbf{y} . First, we determine $\hat{\mathbf{x}} = \mathcal{D}_{VT,n,b,\ell}(a, \mathbf{y})$. From Corollary 10, we have that $\mathbf{x} \in \mathcal{B}_{(T,2\ell)}(\hat{\mathbf{x}})$. Since $\mathbf{x} \in \mathcal{B}_{(T,2\ell)}(\hat{\mathbf{x}})$, we have $d_H(\partial^{-1}(\hat{\mathbf{x}}), \bar{\mathbf{x}}) \leq 2\ell$. Because the minimum distance of the code $\bar{\mathcal{C}}_{(T,\ell)\wedge D}(n, a, b)$ is $4\ell + 1$, we can uniquely recover \mathbf{x} from $\partial^{-1}(\hat{\mathbf{x}})$. ■

Corollary 12. There exists an ℓ -TD code which redundancy at most $2\ell \log n + \log(n + 2\ell + 1)$ bits.

Next, we improve upon this result for the case when $\ell = 1$. Let $a_1, a_2 \in \mathbb{Z}_{n+2L+1}$. Define $\mathbf{Y}_{T\wedge D}(n, a_1, a_2) \subseteq \mathbb{F}_2^n$ according to

$$\mathbf{Y}_{T\wedge D}(n, a_1, a_2) = \{\mathbf{x} : x_n = 0, \sum_{i=1}^{n-1} (2i+1)x_i \equiv a_1 \pmod{n+2L+1}, \sum_{i=1}^{n-1} (2i+1)^2 x_i \equiv a_2 \pmod{n+2L+1}\},$$

where $L \geq 1$ is chosen so that $n + 2L + 1$ is a prime number greater than $2n - 1$. Let

$$\mathcal{C}_{T\wedge D}(n, a_1, a_2) = \mathbf{Y}'_{T\wedge D}(n, a_1, a_2),$$

where \mathbf{Y}' stands for the collection of all derivatives of words in \mathbf{Y} . We have the following lemma.

Lemma 13. For all $a_1, a_2 \in \mathbb{Z}_{n+2L+1}$, the code $\mathcal{C}_{T\wedge D}(n, a_1, a_2)$ is a 1-TD code.

Proof: We use the same approach as the one outlined in the proof of Claim 1.

Since $\sum_{i=1}^{n-1} (2i+1)x_i \equiv a_1 \pmod{n+2L+1}$ and $x_n = 0$, we have that

$$\sum_{i=1}^n i x'_i \equiv a_1 \pmod{n+2L+1}. \quad (3)$$

Furthermore, since $x_n = 0$,

$$\sum_{i=1}^n x'_i \equiv 0 \pmod{2}. \quad (4)$$

From (3) and (4), it is clear that if $\mathbf{x} \in \mathbf{Y}_{T\wedge D}(n, a_1, a_2)$, then $\mathbf{x}' \in \mathcal{C}_{VT}(n, a_1, 0, L)$. Similarly to what was done in Theorem 11, it can be shown that if $L \geq 1$ and $\mathbf{Y}_{T\wedge D}(n, a_1, a_2)$ has

Hamming distance at least 5, then $\mathcal{C}_{T\wedge D}(n, a_1, a_2)$ is a 1-TD code. By design, $L \geq 1$ and so we turn our attention to showing that $\mathbf{Y}_{T\wedge D}(n, a_1, a_2)$ has Hamming distance at least 5.

We claim that the vectors in $\mathbf{Y}_{T\wedge D}(n, a_1, a_2)$ represent a coset of a Berlekamp code [17, Chapter 10.6] with Lee distance 5, which implies the desired result. To prove the claim, note that the binary code $\mathbf{Y}_{T\wedge D}(n, 0, 0)$ has a parity-check matrix of the form

$$H = \begin{bmatrix} 3 & 5 & 7 & \dots & 2n-1 \\ 3^2 & 5^2 & 7^2 & \dots & (2n-1)^2 \end{bmatrix}.$$

According to [17, Chapter 10.6], in order for $\mathbf{Y}_{T\wedge D}(n, 0, 0)$ to have minimum Lee distance 5, the following statement has to be true: For any two columns of H , say h_i and h_j , it has to hold that

$$h_{i_1} + h_{i_2} \neq \begin{bmatrix} 0 \\ c \end{bmatrix},$$

for any possible choice of $c \in \mathbb{F}_{n+2L+1}$. Clearly, this condition is true since $n+2L+1$ is an odd prime and the sum of two odd numbers cannot equal another odd number. Thus, $\mathbf{Y}_{T\wedge D}(n, 0, 0)$ has minimum Lee distance at least 5 and so $\mathbf{Y}_{T\wedge D}(n, a_1, a_2)$ has minimum Lee distance at least 5, as claimed. ■

The above construction improves upon the general construction described by the result (2) in terms of $\log n$ bits of redundancy.

Remark 1. It has been a long standing open problem to find extensions for the single-deletion VT code construction which would have *order optimal* redundancy and impose syndrome constraints of the form $\sum_i f_k(i) x_i \equiv a \pmod{(n+1)}$, for some judiciously chosen functions $f_k(i)$. Attempts based on using this approach have failed so far [3]. On the other hand, the result of Lemma 13 shows that syndrome constraints of the form described above can accommodate combinations of one deletion and other forms of errors, such as adjacent transpositions.

Corollary 14. *There exists a 1-TD code which redundancy at most $2 \log n + c$ bits, for some absolute constant c .*

In the next section, we turn our attention to the problem of constructing codes capable of correcting transposition and deletion errors in the form of blocks of bits. First, we analyze the problem of constructing codes capable of correcting a single block of adjacent deletions. Then, we focus on constructing codes capable of correcting a single transposition of adjacent blocks in addition to handling one block deletion.

V. CODES FOR CORRECTING A BLOCK OF DELETIONS

We describe next a new family of codes capable of correcting one block of at most b consecutive deletions; the codes require $\log b \log n + \mathcal{O}(b^2 \log b \log \log n)$ bits of redundancy, and hence improve upon the state-of-the art scheme which requires at least $(b-1) \log n$ bits of redundancy [19]. The proposed block-deletion codes will subsequently be used in Section VI to construct codes capable of correcting both a block of deletions (which we alternatively refer to a burst of deletions) and an adjacent transposition of two blocks of consecutive symbols.

To explain the intuition behind our approach, we start with a short overview of existing code constructions for correcting a block of consecutive deletions, where the length of the block

is fixed. It will be helpful to think of codewords of length $n = cb$, $c \geq 1$, as two dimensional arrays formed by writing the bits in the codeword column-wise, i.e., by placing the bits (x_1, x_2, \dots, x_b) in an orderly fashion within the first column of the array, the bits $(x_{b+1}, x_{b+2}, \dots, x_{2b})$ within the second column and so on. As an example, for $c = n/b$, the codeword $\mathbf{x} = (x_1, \dots, x_n)$ would read as follows:

$$\begin{bmatrix} x_1 & x_{b+1} & x_{2b+1} & \dots & x_{c(b-1)+1} \\ x_2 & x_{b+2} & x_{2b+2} & \dots & x_{c(b-1)+2} \\ \dots & \dots & \dots & \dots & \dots \\ x_b & x_{2b} & x_{3b} & \dots & x_n \end{bmatrix}. \quad (5)$$

For simplicity, throughout the remainder of this section, we use the term “interleaved sequence” to refer to a row in the array. Note that in this setting, a block of b consecutive deletions in a codeword \mathbf{x} leads to one deletion within each interleaved sequence, and that the locations of deletions in the interleaved sequences are correlated. As an example, the block may cause the same deletion location in the first interleaved sequence, but affect the symbols in the other interleaved sequences differently (The deleted symbols are underlined):

$$\begin{bmatrix} x_1 & x_{b+1} & \underline{x}_{2b+1} & \dots & x_{c(b-1)+1} \\ x_2 & x_{b+2} & \underline{x}_{2b+2} & \dots & x_{c(b-1)+2} \\ \dots & \dots & \dots & \dots & \dots \\ x_b & x_{2b} & \underline{x}_{3b} & \dots & x_n \end{bmatrix}, \quad (6)$$

or

$$\begin{bmatrix} x_1 & x_{b+1} & \underline{x}_{2b+1} & \dots & x_{c(b-1)+1} \\ x_2 & \underline{x}_{b+2} & x_{2b+2} & \dots & x_{c(b-1)+2} \\ \dots & \dots & \dots & \dots & \dots \\ x_b & \underline{x}_{2b} & x_{3b} & \dots & x_n \end{bmatrix}, \quad (7)$$

or

$$\begin{bmatrix} x_1 & x_{b+1} & \underline{x}_{2b+1} & \dots & x_{c(b-1)+1} \\ x_2 & x_{b+2} & \underline{x}_{2b+2} & \dots & x_{c(b-1)+2} \\ \dots & \dots & \dots & \dots & \dots \\ x_b & \underline{x}_{2b} & x_{3b} & \dots & x_n \end{bmatrix}. \quad (8)$$

As a result, by finding the location of the deletion in the first interleaved sequence does not automatically allow one to determine the “shift” of the block with respect to that location. Furthermore, deletion correcting codes such as VT codes only identify the *run* of symbols in which the deletion occurs and not its exact position, as the goal is to reconstruct the correct codeword and not precisely determine the location of the error. As a result, further uncertainty exists about the locations of the deletions in the second, third etc. interleaved sequence of the codeword.

To mitigate these problems, the authors of [5] proposed a construction of codes capable of correcting a block of consecutive deletions of length *exactly* b based on imposing simple constraints on the interleaved sequences of a codeword. A construction with redundancy of approximately $b \log n$ bits requires *all* the interleaved sequences of (18) to belong to a VT code. The main drawback of this construction is that each interleaved sequence is treated independently of the others and that consequently, the redundancy of the codes is too high. To address this problem, one should use the position of the deletion in the first interleaved sequence to approximately determine the

location of the deletion in the second row and similarly for all other subsequent rows. In [5], the authors also proposed a code which has an alternating sequence (i.e., a sequence of the form $0, 1, 0, 1, 0, 1, \dots$) as its first interleaved sequence and all the remaining interleaved sequences satisfying a constraint that requires $\log 3$ bits of redundancy. The proposed code may be easily decoded by first determining the location of the deletion in the first row through a reference to the alternating sequence structure. Then, this location is used by the remaining rows to correct the remaining $b - 1$ deletions. This approach requires at least n/b bits of redundancy, due to the fact that one has to fix the first row of the codeword array. Thus, the redundancy of this approach is actually higher than that of the code that uses individual VT code constraints for each interleaved sequence.

The alternating sequence approach was improved and generalized in [19], where the authors constructed block deletion-correcting codes with a significantly more relaxed constraint placed on the first interleaved sequence. Their idea was to combine constrained coding with a variant of VT codes which we explain in details in what follows. The relaxed constraints allow one to *approximately* determine the locations of the remaining deletions in \mathbf{x} after decoding the first interleaved sequence of the array. The constrained and VT-type constraints imposed on the higher index rows nevertheless allow for unique recovery of the codeword \mathbf{x} by using VT codes confined to the “suspect range” predicted to harbor the deletions. The codes constructed in [19] require approximately $\log n$ bits of redundancy for the constraint in the first row of the array, and $\log \log n$ bits of redundancy for each of the remaining rows. This results in a total redundancy of roughly $\log n + (b - 1) \log \log n$ bits for correcting a block of consecutive deletions of length exactly b (compared to the redundancy of [5] which equals $b \log n$ bits).

To allow for correcting any single block of length at most b , the codes from [19] have to be changed so as to include nested redundant bits that capture multiple coding constraints and may allow for correcting a range of block lengths. Which of the constraints to use is apparent upon observing the length of the received word: To correct one block of any possible length at most b , the decoder for the underlying code locates the position of the block of consecutive deletions differently for each possible block length. For instance, if \mathbf{x} experiences a block error of length $b_1 \leq b$, then the code uses one VT-type constraint, say K_{VT, b_1} . However, if \mathbf{x} experiences an error burst of length b_2 with $b_2 < b_1$, then the code effectively uses a different VT-type constraint, say K_{VT, b_2} . Note that since each of the constraints K_{VT, b_i} , $2 \leq i \leq b$, is de facto a VT-type constraint, one requires roughly $(b - 1) \log n + b^2 \log \log n$ bits of redundancy, compared to the $b^2 \log n$ redundancy which would have been required by the scheme in [5].

Our approach in this work for a further improvement is to reuse the same VT-type constraint for multiple possible block lengths, in which case the redundancy will amount to roughly $\log b \log n + \log b b^2 \log \log n$ bits. To describe this method, we start with a construction that allows for correcting one odd-length block of consecutive deletions of length at most b , and then proceed to extend the result for even-length blocks.

A. Odd Length Blocks

Our code construction is centered around three main ideas:

- 1) The use of VT codes (10).
- 2) The use of running sum constraint (12).
- 3) The use of a sequence of *Shifted VT codes* [19], defined in (15) i.e., codes that enforce multiple modular VT-type constraints with parameter values smaller than $n + 1$.

As discussed in more details in what follows, our choice of the Shifted VT codes requires approximately $b^2 \log \log n$ bits of redundancy and the constrained coding constraint requires a single bit of redundancy, the proposed construction introduces roughly $\log n + b^2 \log \log n$ bits of redundancy.

The decoder operates as follows. Suppose that \mathbf{y} is the result of deleting t consecutive bits from \mathbf{x} , with $t \leq b$ and t odd. Then,

- 1) The decoder computes a number of parities and decides on the appropriate Shifted VT code (15) to use in determining the Hamming weight of the bits deleted from \mathbf{x} .
- 2) Using both the VT-type constraint (10) and the constraint (12), the decoder determines an approximate location for the block deletion in \mathbf{x} that resulted in \mathbf{y} .
- 3) Given the approximate location of the block of deletions, the decoder uses a series of Shifted VT codes (15) to determine the exact locations and values of the bits deleted from \mathbf{x} that lead to \mathbf{y} .

Part 1. Determining the weight of the deleted substring.

We start with some relevant terminology and notation. For a word $\mathbf{x} \in \mathbb{F}_2^n$, let $\mathcal{B}_{D, \leq b}(\mathbf{x})$ denote the set of all words that may be obtained from \mathbf{x} by deleting at most b consecutive bits. For example, for $\mathbf{x} = (0, 1, 1, 0, 0, 1) \in \mathbb{F}_2^6$, we have

$$\mathcal{B}_{D, \leq 2}(\mathbf{x}) = \left\{ (0, 1, 1, 0, 0, 1), (1, 1, 0, 0, 1), (0, 1, 0, 0, 1), \right. \\ \left. (0, 1, 1, 0, 1), (0, 1, 1, 0, 0), (1, 0, 0, 1), (0, 0, 0, 1), \right. \\ \left. (0, 1, 0, 1), (0, 1, 1, 1), (0, 1, 1, 0) \right\}.$$

Similarly, let $\mathcal{B}_{D, b}(\mathbf{x})$ denote the set of words that may be obtained from \mathbf{x} by deleting *exactly* b consecutive bits.

Furthermore, given a vector $\mathbf{d} \in \mathbb{F}_2^b$, define the code $\mathcal{C}_{par}(n, b, \mathbf{d})$ as follows²:

$$\mathcal{C}_{par}(n, b, \mathbf{d}) = \left\{ \mathbf{x} \in \mathbb{F}_2^n : \forall j \in [b], \sum_{i=1}^{\lceil \frac{n-j+1}{b} \rceil} x_{j+bi} \equiv d_j \pmod{2} \right\}.$$

It is straightforward to see that the code imposes a single parity-check constraint on the interleaved sequences of \mathbf{x} , which suffices to determine the weight of the deleted block. In addition, we observe that we used a set of parameters d_i for the weight constraints, rather than the classical even parity constraints for reasons that will become apparent in the subsequent exposition. In a nutshell, the resulting codes of the section will be nonlinear and averaging arguments for the size of codes require the use of a range of parameter values.

²We use the subscript *par* to refer to the function of the code, which is to recover the weight of the deleted block (substring) by using simple parity checks.

Example 6. Suppose that $\mathbf{x} = (0, 1, 1, 0, 0, \mathbf{1}, 0, 1, 0, 1, 0, 1) \in \mathcal{C}_{par}(12, 2, (1, 1))$ was transmitted and $\mathbf{y} = (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \in \mathcal{B}_{D,2}(\mathbf{x})$ was received instead. Since $\mathbf{x} \in \mathcal{C}_{par}(12, 2, (1, 1))$, it is straightforward to determine that the bits 0, 1 were deleted from \mathbf{x} to obtain \mathbf{y} . Notice, however, that we cannot infer the order in which the deleted bits $\{0, 1\}$ appeared in \mathbf{x} from the constraints of the code $\mathcal{C}_{par}(12, 2, (1, 1))$, nor their exact location.

Part 2. Imposing the generalized VT conditions.

Given $\mathbf{y} \in \mathbb{F}_2^{n-b}$, $\mathbf{v} \in \mathbb{F}_2^b$ and $k_I \in [n - b + 1]$, let $I(\mathbf{y}, \mathbf{v}, k_I) \in \mathbb{F}_2^n$ be the vector obtained by inserting \mathbf{v} into \mathbf{y} at position k_I . For instance, if $\mathbf{y} = (0, 1, 1, 0, 0, 1) \in \mathbb{F}_2^6$, $k_I = 1$ and $\mathbf{v} = (0, 1)$, then $I(\mathbf{y}, \mathbf{v}, 1) = (\mathbf{0}, \mathbf{1}, 0, 1, 1, 0, 0, 1) \in \mathbb{F}_2^8$. Similarly, let $D(\mathbf{y}, b, k_D)$ be the result of deleting b consecutive bits from \mathbf{y} starting at position k_D . Thus, $D(\mathbf{y}, 2, 2) = (0, 0, 0, 1) \in \mathbb{F}_2^4$. As before, let $wt(\mathbf{x})$ stand for the Hamming weight of a vector \mathbf{x} .

Claim 3. Let $\mathbf{v}_1, \mathbf{v}_2 \in \mathbb{F}_2^b$, and suppose that $\mathbf{y} \in \mathbb{F}_2^{n-b}$ and that $w_1 = wt(\mathbf{v}_1) = wt(\mathbf{v}_2)$, $w_2 = wt(y_{i_1}, \dots, y_{i_2-1})$, where $i_1 < i_2$. Let $\mathbf{x} = I(\mathbf{y}, \mathbf{v}_1, i_1) \in \mathbb{F}_2^n$ and $\mathbf{u} = I(\mathbf{y}, \mathbf{v}_2, i_2) \in \mathbb{F}_2^n$. Then,

$$\sum_{i=1}^n iu_i - \sum_{i=1}^n ix_i = (i_2 - i_1)w_1 - bw_2 + \delta, \quad (9)$$

where $|\delta| < b^2$.

Remark 2. Note that the term δ arises due to the fact that the sequences \mathbf{v}_1 and \mathbf{v}_2 have the same weight but potentially different locations of their nonzero symbols.

Let $\mathcal{C}_{VT,b}(n, a, b)$ be a VT code of the form

$$\mathcal{C}_{VT,b}(n, a, b) = \{\mathbf{x} \in \mathbb{F}_2^n : \sum_{i=1}^n ix_i \equiv a \pmod{(bn + b^2)}\}. \quad (10)$$

Clearly, two vectors \mathbf{x} and \mathbf{u} of the form as defined in Claim 3 cannot both lie in the same code capable of correcting a block of deletions of length at most b . To see this, note that $\mathbf{y} = D(\mathbf{x}, b, i_1) = D(\mathbf{u}, b, i_2) \in \mathcal{B}_{D,b}(\mathbf{x}) \cap \mathcal{B}_{D,b}(\mathbf{u})$, a contradiction.

If we assume that $\mathbf{x}, \mathbf{u} \in \mathcal{C}_{VT,b}(n, a, b)$ are typical sequences generated by an i.i.d uniform source, then, with high probability, w_2 will be close in value to $\frac{i_2 - i_1}{2}$. In order for \mathbf{x} and \mathbf{u} to belong to different codes (i.e., codes with different VT syndromes) capable of correcting block deletions of length at most b for an overwhelming large portion of the constituent vectors \mathbf{v} , based on Claim 3 and the definition of $\mathcal{C}_{VT,b}(n, a, b)$, we need to ensure that the right-hand side of (9) is not zero, i.e., that

$$(i_2 - i_1)w_1 + \delta \neq b \frac{i_2 - i_1}{2}. \quad (11)$$

Note that if b is odd, then w_1 cannot be equal to $b/2$.

Next, we construct a codebook that ensures that (11) is satisfied for any choice of distinct (code)words. The idea is to construct a set of codewords \mathbf{x} with the following property: Every block (substring) in \mathbf{x} of length $i_2 - i_1 = B$, where $B \geq b^4 \log n$, has to have Hamming weight approximately equal to $\frac{B}{2}$. If every block of $B \geq b^4 \log n$ bits in \mathbf{x} has weight close

to $B/2$ and if b is odd, then one can show (see Lemma 15) that for any i_1, i_2 such that $i_2 - i_1 \geq B$, \mathbf{x}, \mathbf{u} do not both belong to the same VT code. Therefore, when a block of deletions occurs, Lemma 15 shows that it will be possible to determine approximately (to within B bits) the location of the block of deletions by attempting to insert a block of bits into different positions and check whether they lead to a vector that satisfies a VT-type constraint. According to Lemma 15, if the VT-type constraint is satisfied, we know the location of the block of deletions to within B positions and we can determine exactly the value and location of the deleted bits using the Shifted VT codes in (15).

For notational convenience, we henceforth assume that n is a power of two so that $\log n$ is a positive integer. Let $Bal(n, b)$ denote the following “balanced” set of sequences:

$$Bal(n, b) = \left\{ \mathbf{x} \in \mathbb{F}_2^n : \forall B \in [n], B \geq b^4 \log n, \forall j \in [n - B + 1], \right. \\ \left. \frac{B}{2} - \frac{B}{3b} < \sum_{i=j}^{j+B-1} x_i < \frac{B}{2} + \frac{B}{3b} \right\}. \quad (12)$$

We have the following claim, the proof of which may be found in Appendix A.

Claim 4. For a positive integer $n \geq 10$ and $b \geq 5$,

$$\log |Bal(n, b)| \geq n + \log \left(1 - 2n^{2-\frac{2}{3}b^2 \log e} \right).$$

Note that as a consequence of Claim 4, we have

$$\log |Bal(n, b)| \geq n - 1, \quad (13)$$

and the coding constraint incurs not more than one bit of redundancy.

Let $\mathbf{D} = (d_1, d_2, \dots, d_b)$, where for $i \in [b]$, $d_i = (d_{1,i}, \dots, d_{i,i}) \in \mathbb{F}_2^i$. Define

$$\mathcal{C}_b^{odd}(n, a, \mathbf{D}) = \left\{ \mathbf{x} \in \mathbb{F}_2^n : \sum_{i=1}^n ix_i \equiv a \pmod{bn + b^2}, \right. \\ \left. \mathbf{x} \in Bal(n, b), \forall i \in [b] \right. \\ \left. \mathbf{x} \in \mathcal{C}_{par}(n, i, d_i) \right\}.$$

We show next that if \mathbf{y} is the result of an odd-length block of deletions occurring in $\mathbf{x} \in \mathcal{C}_b^{odd}(n, a, \mathbf{D})$ starting at position k_D , then there exists a decoder for $\mathcal{C}_b^{odd}(n, a, \mathbf{D})$ that is capable of producing an estimate, say \hat{k}_D , for the starting position of the block of deletions, with $|k_D - \hat{k}_D| < b^4 \log n$. We then proceed to explain how to recover the exact value and location of the deleted bits using the SVT codes of (15).

First, we show that if $\mathbf{y} \in \mathcal{B}_{D,t}(\mathbf{x})$ and $\mathbf{x} \in \mathcal{C}_b^{odd}(n, a, \mathbf{D})$, with $t \leq b$ an odd integer, one can obtain a good estimate for the location of the block of deletions given that we know the Hamming weight of the bits that were deleted (we can obtain this from a decoder for the subcode $\mathcal{C}_{par}(n, i, d_i)$). The following result, similar to Claim 3, describes the relevant properties of the decoder.

Lemma 15. Let $\mathbf{v}_1, \mathbf{v}_2 \in \mathbb{F}_2^t$, $wt(\mathbf{v}_1) = wt(\mathbf{v}_2)$, $\mathbf{y} \in \mathbb{F}_2^{n-t}$, and suppose that t is an odd number where $t \leq b$ and $b \geq 5$. For $i_1 <$

i_2 and $i_2 - i_1 \geq b^4 \log n$, let $\mathbf{x} = I(\mathbf{y}, \mathbf{v}_1, i_1) \in \mathcal{C}_b^{\text{odd}}(n, a, \mathbf{D})$ and $\mathbf{z} = I(\mathbf{y}, \mathbf{v}_2, i_2) \in \mathbb{F}_2^n$. Then,

$$\sum_{i=1}^n i z_i - \sum_{i=1}^n i x_i \not\equiv 0 \pmod{bn + b^2},$$

and hence $\mathbf{z} \notin \mathcal{C}_b^{\text{odd}}(n, a, \mathbf{D})$.

Proof: As before, let $w_1 = wt(\mathbf{v}_1) = wt(\mathbf{v}_2)$ and $w_2 = wt(y_{i_1}, \dots, y_{i_2-1})$. Now according to Claim 3,

$$\sum_{i=1}^n i z_i - \sum_{i=1}^n i x_i = Bw_1 - tw_2 + \delta,$$

and therefore our goal is to show that

$$Bw_1 + \delta \not\equiv tw_2 \pmod{bn + b^2}, \quad (14)$$

whenever $B = i_2 - i_1 \geq b^4 \log n$, which will establish the statement of the lemma.

Since $\mathbf{x} \in \mathcal{C}_b^{\text{odd}}(n, a, \mathbf{D})$, one has $\mathbf{x} \in \text{Bal}(n, b)$ and hence it follows from (12) that

$$\frac{B}{2} - \frac{B}{3b} < \sum_{i=i_1}^{i_2-1} y_i < \frac{B}{2} + \frac{B}{3b}.$$

Thus, given that $t \leq b$,

$$\frac{Bt}{2} - \frac{B}{3} < tw_2 < \frac{Bt}{2} + \frac{B}{3}.$$

Notice that since t is odd, and since $w_1 = (t+k)/2$, where $-b \leq k \leq b$, k is odd. Thus, we have

$$Bw_1 + \delta = \frac{Bt}{2} + k \frac{B}{2} + \delta,$$

where $k \neq 0$. We will prove the result for the case when k is positive. The result may be proved similarly for negative k . For $k \geq 1$, we have

$$Bw_1 + \delta \geq \frac{Bt}{2} + \frac{B}{2} - b^2.$$

Since $B \geq b^4 \log n$ and $b \geq 5$, it follows that

$$Bw_1 + \delta \geq \frac{Bt}{2} + \frac{B}{2} - b^2 > \frac{Bt}{2} + \frac{B}{3} > tw_2,$$

and hence (14) holds. \blacksquare

The desired code $\mathcal{C}_b^{\text{odd}}(n, a, \mathbf{C}, \mathbf{D}) \subseteq \mathbb{F}_2^n$, capable of correcting any single block of odd length $t \leq b$, is a subcode of the code $\mathcal{C}_b^{\text{odd}}(n, a, \mathbf{D}) \subseteq \mathbb{F}_2^n$. From Lemma 15, we know that the code $\mathcal{C}_b^{\text{odd}}(n, a, \mathbf{D})$ can approximately determine the location of the block of deletions, assuming the block is odd. In what follows, we describe Shifted VT codes which will be used in Part 4 to exactly pinpoint the locations and values of the deleted symbols.

Part 3. Incorporating Shifted VT codes. We now briefly turn our attention to Shifted VT codes introduced in [19]. For completeness, we state the results necessary for our subsequent derivations and provide an example of the decoding process. For further details, see Appendix B.

The Shifted VT code with positive integer parameters c, d and n, M , denoted $SVT_{c,d}(n, M)$, is defined as follows:

$$SVT_{c,d}(n, M) = \{\mathbf{x} \in \mathbb{F}_2^n : \sum_{i=1}^n i x_i \equiv c \pmod{M}, \sum_{i=1}^n x_i \equiv d \pmod{2}\}. \quad (15)$$

A Shifted VT code is capable of determining the exact location and value of a bit deleted from a codeword provided some sufficiently accurate estimate for the location of the deletion is known. To see why this is true, observe that the modulus of the sum in the definition equals M , which is assumed to be significantly smaller than $n+1$, the modulus used in classical VT codes. The code basically imposes a VT-type constraint, which can correct a single deletion error, but on a substring of the sequence. This code property is described more precisely in the next lemma.

Lemma 16. Suppose that $\mathbf{y} \in D(\mathbf{x}, 1, k_D)$, where $\mathbf{x} \in SVT_{c,d}(n, M)$ and where $M \geq 2P - 1$, $d_b \in \mathbb{F}_2$. Given a \hat{k}_D such that $|k_D - \hat{k}_D| < P$, there exists at most one possible value for k'_D and for d_b that jointly satisfy $I(\mathbf{y}, d_b, k'_D) \in SVT_{c,d}(n, M)$. In this setting, we have $I(\mathbf{y}, d_b, k'_D) = \mathbf{x}$.

Example 7. Suppose that $\mathbf{x} = (0, 1, \mathbf{1}, 0, 0, 1) \in SVT_{2,1}(6, 2P-1)$, $\mathbf{y} = D(\mathbf{x}, 1, 3) = (0, 1, 0, 0, 1)$, $\hat{k}_d = 4$, and $P = 2$. Note that in the example, $k_d = 3$ so that $|\hat{k}_d - k_d| < P$, as required by the setup of Lemma 16.

Clearly, we can determine the value of the deleted bit to be 1, given that \mathbf{y} and $\sum_{i=1}^6 x_i \equiv 1 \pmod{2}$. Thus, we conclude that $k_d \in \{2, 3, 4\}$ since the decoder for $SVT_{2,1}(6, 2P-1)$ provided the estimate $\hat{k}_d = 4$, and we already had the prior knowledge that $|\hat{k}_d - k_d| < P$. To proceed, we need to examine each of the following three deletion locations, as shown below:

$$\hat{\mathbf{x}}_1 = (0, 1, \mathbf{1}, 0, 0, 1), \text{ for } k_d = 3,$$

$$\hat{\mathbf{x}}_2 = (0, 1, 0, \mathbf{1}, 0, 1), \text{ for } k_d = 4,$$

$$\hat{\mathbf{x}}_3 = (0, 1, 0, 0, \mathbf{1}, 1), \text{ for } k_d = 5.$$

Observe that $\hat{\mathbf{x}}_1 \in SVT_{2,1}(6, 3)$, $\hat{\mathbf{x}}_2 \in SVT_{0,1}(6, 3)$, $\hat{\mathbf{x}}_3 \in SVT_{1,1}(6, 3)$. Thus, the decoder for $SVT_{2,1}(6, 3)$ can conclude that $\mathbf{x} = \hat{\mathbf{x}}_1$, since this is the only one of the three vectors that belongs to the code $SVT_{2,1}(6, 3)$.

Part 4. Combining the different code construction components. Next, we describe a family of codes $\mathcal{C}_b^{\text{odd}}(n, a, \mathbf{C}, \mathbf{D})$, capable of correcting any odd-length block of consecutive deletions of length not exceeding b .

Let $\mathbf{D} = (d_1, d_2, \dots, d_b)$, where for $i \in [b]$, $d_i = (d_{1,i}, \dots, d_{i,i}) \in \mathbb{F}_2^i$. Furthermore, let $\mathbf{C} = (c_1, c_2, \dots, c_b)$ where for $i \in [b]$, $c_i = (c_{1,i}, \dots, c_{i,i}) \in \mathbb{Z}_{2b^5 \log n}^i$. For a vector $\mathbf{x} \in \mathbb{F}_2^n$, let $\mathbf{x}^{(f,b)}$ be the f -th interleaved sequence of \mathbf{x} . For instance if $\mathbf{x} = (0, 1, \mathbf{1}, 0, 0, 1)$, then $\mathbf{x}^{(1,2)} = (0, \mathbf{1}, 0)$. Similarly, $\mathbf{x}^{(2,2)} = (1, 0, 1)$.

We define a code $\mathcal{C}_b^{odd}(n, a, \mathbf{C}, \mathbf{D}) \subseteq \mathbb{F}_2^n$ as follows³:

$$\begin{aligned} \mathcal{C}_b^{odd}(n, a, \mathbf{C}, \mathbf{D}) = \left\{ \mathbf{x} \in \mathbb{F}_2^n : \sum_{i=1}^n i x_i \equiv a \pmod{bn + b^2}, \right. \\ \left. \mathbf{x} \in \text{Bal}(n, b), \text{ and } \forall i_2 \in [b], \forall i_1 \leq i_2, \right. \\ \left. \mathbf{x}^{(i_1, i_2)} \in \text{SVT}_{c_{i_1, i_2}, d_{i_1, i_2}} \left(\left\lceil \frac{n - i_1 + 1}{i_2} \right\rceil, 2b^5 \log n \right) \right\}, \end{aligned} \quad (16)$$

where the $d_{i,j}$ s are elements of the vectors \mathbf{d}_i defined above.

Intuitively, the code $\mathcal{C}_b^{odd}(n, a, \mathbf{C}, \mathbf{D})$ ensures that the VT and balancing constraints are satisfied, and introduces the SVT-type constraint that allows one to determine the exact location of a block error given a sufficiently close estimate of the correct location. Note that $\mathcal{C}_b^{odd}(n, a, \mathbf{C}, \mathbf{D}) \subseteq \mathcal{C}_b^{odd}(n, a, \mathbf{D})$, and in particular, if $\mathbf{x} \in \text{SVT}_{c_{i_1, i_2}, d_{i_1, i_2}}(n, 2b^5 \log n)$ for $i_1 \leq i_2$, then $\mathbf{x} \in \mathcal{C}_{par}(n, i_2, \mathbf{d}_{i_2})$.

Theorem 17. Suppose that $\mathbf{x} \in \mathcal{C}_b^{odd}(n, a, \mathbf{C}, \mathbf{D})$ and that $\mathbf{y} \in \mathcal{B}_{D,t}(\mathbf{x})$, where t is an odd integer such that $t \leq b$, $b \geq 5$. Then, there exists a decoder for $\mathcal{C}_b^{odd}(n, a, \mathbf{C}, \mathbf{D})$ that can recover \mathbf{x} from \mathbf{y} .

Proof: Assume that $\mathbf{y} = D(\mathbf{x}, t, k_D)$ and let $\mathbf{v} = (x_{k_D}, x_{k_D+1}, \dots, x_{k_D+t-1})$. First, we use the fact that $\mathbf{x} \in \mathcal{C}_{par}(n, t, \mathbf{d}_t)$, which follows from the constraint that $\mathbf{x} \in \text{SVT}_{c_{i_1, i_2}, d_{i_1, i_2}}(\lceil \frac{n-i_1+1}{i_2} \rceil, 2b^5 \log n)$, to determine the precise values of the deleted bits. For this purpose, let w denote the number of deleted nonzero symbols. Clearly, $wt(\mathbf{v}) = w$.

Next, we determine $\hat{\mathbf{v}} \in \mathbb{F}_2^t$ and a $\hat{k}_D \in [n - t + 1]$ such that $wt(\hat{\mathbf{v}}) = w$ and $I(\mathbf{y}, \hat{\mathbf{v}}, \hat{k}_D) \in \mathcal{C}_b^{odd}(n, a, \mathbf{D})$. Since $I(\mathbf{y}, \mathbf{v}, k_D) \in \mathcal{C}_b^{odd}(n, a, \mathbf{C}, \mathbf{D})$ and $wt(\mathbf{v}) = wt(\hat{\mathbf{v}})$, it follows from Lemma 15 that if $I(\mathbf{y}, \hat{\mathbf{v}}, \hat{k}_D) \in \mathcal{C}_b^{odd}(n, a, \mathbf{D})$, then $|k_D - \hat{k}_D| < b^4 \log n$. Finally, we use the constraint $\mathbf{x} \in \text{SVT}_{c_{i_1, i_2}, d_{i_1, i_2}}(\lceil \frac{n-i_1+1}{i_2} \rceil, 2b^5 \log n)$ once again to recover the exact locations and values of the deleted bits. ■

Example 8. Suppose that $\mathbf{x} = (0, 1, 1, \mathbf{0, 0}, 1, 1, 0, 0, 1, 1, 0)$, so that $\mathbf{x} \in \mathcal{C}_{par}(13, 3, (1, 1, 0))$ and $\sum_{i=1}^{13} i x_i \equiv 43 \pmod{48}$. If $\mathbf{y} = (0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \in \mathcal{B}_{D,3}(\mathbf{x})$, then there exists only one vector $\hat{\mathbf{x}} = (\hat{x}_1, \dots, \hat{x}_n)$ such that $\hat{\mathbf{x}} \in \mathcal{C}_{par}(13, 3, (1, 1, 0))$ and $\sum_{i=1}^{13} i x_i \equiv 43 \pmod{48}$, namely $\hat{\mathbf{x}} = \mathbf{x}$.

Corollary 18. Let $\mathbf{x}, \mathbf{u} \in \mathcal{C}_b^{odd}(n, a, \mathbf{C}, \mathbf{D}) \subseteq \mathbb{F}_2^n$, where $\mathbf{x} \neq \mathbf{u}$ and let t be an odd integer such that $t \leq b$ and $b \geq 5$. Then, $\mathcal{B}_{D,t}(\mathbf{x}) \cap \mathcal{B}_{D,t}(\mathbf{u}) = \emptyset$, and for any $n \geq 10$, $\mathcal{C}_b^{odd}(n, a, \mathbf{C}, \mathbf{D})$ has at most

$$\log(bn + b^2) + \frac{b(b+1)}{2} (\log(2b^5 \log n) + 1) + 1$$

bits of redundancy.

The result concerning the cardinality of the code follows from a straightforward averaging argument. The proof of the result can be found in Appendix C.

³The superscript *odd* is used to indicate the fact that the length of the block of deletions is odd.

B. The general case

We now turn our attention to extending the previous construction so that it applies to blocks of arbitrary length – odd or even – not exceeding b . The gist of the approach is to decompose a block of length b into odd blocks, when viewed through the interleaved sequences of \mathbf{x} . The next example illustrates how this will be accomplished.

Example 9. Suppose that $\mathbf{x} = (\mathbf{0, 0, 1, 0, 1, 0}, 0, 1, 0) \in \mathbb{F}_2^9$ is transmitted and that the vector $\mathbf{y} = (0, 1, 0) \in \mathcal{B}_{D,6}(\mathbf{x})$ is received instead. Notice that in this case, the sequence $\mathbf{x}^{(1,2)} = (\mathbf{0, 1, 1}, 0, 0)$ experienced an odd block of consecutive deletions of length three, resulting in $\mathbf{y}^{(1,2)} = (0, 0)$.

Define the codebook $\mathcal{C}_b(n, \mathbf{a}, \vec{\mathbf{C}}, \vec{\mathbf{D}})$ according to

$$\begin{aligned} \mathcal{C}_b(n, \mathbf{a}, \vec{\mathbf{C}}, \vec{\mathbf{D}}) = \left\{ \mathbf{x} \in \mathbb{F}_2^n : \right. \\ \left. \forall j \in [\lceil \log b \rceil], \mathbf{x}^{(1, 2^{j-1})} \in \mathcal{C}_b^{odd}(\lceil \frac{n}{2^{j-1}} \rceil, a_j, \mathbf{C}_j, \mathbf{D}_j) \right. \\ \left. \text{where } \tilde{b} = \max\{\lceil \frac{b}{2^{j-1}} \rceil, 5\} \right\}, \end{aligned} \quad (17)$$

where $\mathbf{a} = (a_1, \dots, a_{\lceil \log b \rceil})$, $\vec{\mathbf{C}} = (\mathbf{C}_1, \dots, \mathbf{C}_{\lceil \log b \rceil})$, $\vec{\mathbf{D}} = (\mathbf{D}_1, \dots, \mathbf{D}_{\lceil \log b \rceil})$, and where the codes $\mathcal{C}_b^{odd}(\lceil \frac{n}{2^{j-1}} \rceil, a_j, \mathbf{C}_j, \mathbf{D}_j)$ are as defined in (16).

Let $\mathbf{y} = D(\mathbf{x}, t, k_D) \in \mathcal{B}_{D, \leq b}(\mathbf{x})$. Similarly to what was done in the context of odd blocks, we first produce an estimate \hat{k}_D for k_D . Suppose that $t = 2^{j-1}(2l+1)$. We use the constraint $\mathbf{x}^{(1, 2^{j-1})} \in \mathcal{C}_b^{odd}(\lceil \frac{n}{2^{j-1}} \rceil, a_j, \mathbf{C}_j, \mathbf{D}_j)$ to determine the sequence $\mathbf{x}^{(1, 2^{j-1})}$, and use this information to compute \hat{k}_D . Subsequently, using \hat{k}_D and the SVT code constraints, we can determine the correct locations and values of the deleted bits.

We say that $\mathbf{v} \in \mathbb{F}_2^B$ is a b -repeating pattern of length B if for any $1 \leq k \leq \lfloor B/b \rfloor$, we have $(v_1, \dots, v_b) = (v_{bk+1}, \dots, v_{b(k+b)})$. For instance $\mathbf{v} = (0, 1, 1, 0, 1, 1)$ is a 3-repeating pattern of length 6. We find the following claim useful for the proof of the main result of this section.

Claim 5. Suppose that $\mathbf{v} \in \mathbb{F}_2^B$ is a b -repeating pattern of length B , with b odd, that appears as a substring in $\mathbf{x} \in \text{Bal}(n, b)$. Then, $B < b^4 \log n$.

Proof: The result claims that self-repeating patterns in codewords \mathbf{x} of the code under consideration have to be sufficiently short. To prove the claim, suppose that on the contrary, there exists a b -repeating pattern $\mathbf{v} \in \mathbb{F}_2^B$ in $\mathbf{x} \in \text{Bal}(n, b)$ such that $B \geq b^4 \log n$. Let $wt(v_1, \dots, v_b) = (b+k)/2$ where, since b is odd, k is odd. In particular, $k \neq 0$. Then,

$$\sum_{i=1}^B v_i = \frac{b+k}{2} B = \frac{B}{2} + \frac{Bk}{2b},$$

and we arrive at a contradiction since in this case \mathbf{v} cannot be a substring of $\mathbf{x} \in \text{Bal}(n, b)$. ■

The b -repeating patterns serve the same role as runs in the single deletion case when applied to a block of consecutive deletions. Hence, a VT-type code can only determine in which b -repeating pattern the deletions occurred, but not the exact position of the block. This observation is illustrated by the following example.

Example 10. Suppose that the vector $\mathbf{x} = (0, 1, 1, \mathbf{0, 1, 1}, 0, 0, 1) \in \mathcal{C}$ was transmitted and that the vector $\mathbf{y} = (0, 1, 1, 0, 0, 1)$ was received. Note that given \mathbf{x} and \mathbf{y} , it is possible to determine that the substring $(\mathbf{0, 1, 1})$ was deleted from \mathbf{x} to generate \mathbf{y} . However, observe that $\mathbf{x} = I(\mathbf{y}, (0, 1, 1), 1) = (\mathbf{y}, (0, 1, 1), 4)$, where both positions 1 and 4 are contained within a b -repeating pattern of length 6.

We are now ready to state the main result of the section.

Theorem 19. Suppose that $\mathbf{x} \in \mathcal{C}_b(n, \mathbf{a}, \vec{\mathbf{C}}, \vec{\mathbf{D}})$, where $b \geq 5$ is odd, is transmitted, and that $\mathbf{y} \in \mathcal{B}_{D, \leq b}(\mathbf{x}) = D(\mathbf{x}, t, k_D)$, where $1 \leq t \leq b$, is received instead. Then there exists a decoder for $\mathcal{C}_b(n, \mathbf{a}, \vec{\mathbf{C}}, \vec{\mathbf{D}})$ capable of uniquely determining \mathbf{x} from \mathbf{y} .

Note that the assumption that b is odd is made for simplicity of analysis, and that all number of errors $t \leq b$ may be corrected independent on their parity.

Proof: Suppose that \mathbf{y} has length $n - t$, where t is an odd integer. Then, the result immediately follows from the fact that $\mathbf{x} = \mathbf{x}^{(1, 2^0)} \in \mathcal{C}_b^{\text{odd}}(n, a_1, \mathbf{C}_1, \mathbf{D}_1)$ and Theorem 17.

Suppose next that $t = 2^{j-1}(2l+1)$ for some positive integer j and $l \geq 0$. Since

$$\mathbf{x} \in \mathcal{C}_b(n, \mathbf{a}, \vec{\mathbf{C}}, \vec{\mathbf{D}}),$$

we know that

$$\mathbf{x}^{(1, 2^{j-1})} \in \mathcal{C}_b^{\text{odd}}(\lceil \frac{n}{2^{j-1}} \rceil, a_j, \mathbf{C}_j, \mathbf{D}_j),$$

where j, \tilde{b} are as stated in the claim. Thus, it is possible to determine $\mathbf{x}^{(1, 2^{j-1})}$ from $\mathbf{y}^{(1, 2^{j-1})}$ since $\mathbf{y}^{(1, 2^{j-1})} \in \mathcal{B}_{D, 2l+1}(\mathbf{x}^{(1, 2^{j-1})})$. Note that from $\mathbf{x}^{(1, 2^{j-1})}$ and $\mathbf{y}^{(1, 2^{j-1})}$, we can determine the $(2l+1)$ -repeating pattern in which the deletions occurred in $\mathbf{x}^{(1, 2^{j-1})}$ so as to produce $\mathbf{y}^{(1, 2^{j-1})}$.

Assume now that $\mathbf{y}^{(1, 2^{j-1})} = D(\mathbf{x}^{(1, 2^{j-1})}, 2l+1, k'_D)$, and that the goal is to produce an estimate for k'_D , the starting location of the block of deletions. Suppose that the $(2l+1)$ -repeating pattern identified in the above analysis starts at position k''_D in $\mathbf{x}^{(1, 2^{j-1})}$. Since any $(2l+1)$ -repeating pattern which appears as a substring in \mathbf{x} has length less than $b^4 \log n$ according to Claim 5, $|k'_D - k''_D| < b^4 \log n$. Then, $\hat{k}_D = 1 + 2^{j-1}(k''_D - 1)$ satisfies $|\hat{k}_D - k_D| < b^5 \log n$. Therefore, since $\mathbf{x} \in \mathcal{C}_b^{\text{odd}}(n, a_j, \mathbf{C}_j, \mathbf{D}_j)$, we can recover \mathbf{x} from \mathbf{y} by using the constraint $\mathbf{x}^{(i_1, i_2)} \in SVT_{c_{i_1, i_2}, d_{i_1, i_2}}(\lceil \frac{n-i_1+1}{i_2} \rceil, 2b^5 \log n)$, along with the information about \hat{k}_D . ■

The next corollary summarizes the results of this section.

Corollary 20. Let $\mathbf{x}, \mathbf{u} \in \mathcal{C}_b(n, \mathbf{a}, \vec{\mathbf{C}}, \vec{\mathbf{D}}) \subseteq \mathbb{F}_2^n$ where $\mathbf{x} \neq \mathbf{u}$ and let t be a positive integer such that $t \leq b$ for an odd positive integer $b \geq 5$. Then, $\mathcal{B}_{D, t}(\mathbf{x}) \cap \mathcal{B}_{D, t}(\mathbf{u}) = \emptyset$, and for any $n \geq 50b$, the code $\mathcal{C}_b(n, \mathbf{a}, \vec{\mathbf{C}}, \vec{\mathbf{D}})$ introduces at most

$$\lceil \log b \rceil \left(\log(bn + b^2) + \frac{b(b+1)}{2} (\log(2b^5 \log n) + 1) \right) + 1$$

bits of redundancy.

The proof of the result proceeds along the same lines as that of Corollary 18 and may be found in Appendix D.

Remark. It is tedious, but conceptually simple, to extend the results for a single deletion and multiple adjacent transposition errors for the case of multiple deletions and multiple adjacent transpositions, even for the case of a non-binary alphabet. The key idea is to replace VT-like codes with binary codes constructed in [12] and the extensions of the construction over larger fields, as presented in [1]. In the former case, the VT-type constraints are replaced by what the authors refer to as number-theoretic constraints of the form

$$\sum_{i=1}^n v_i x_i = a \pmod{u},$$

where the weights v are defined recursively according to the formula

$$v_j = 1 + \sum_{i=1}^s v_{j-i}, \quad v_i = 0, \quad \forall i \leq 0,$$

and

$$u = 1 + \sum_{i=0}^{s-1} v_{n-i}.$$

VI. CODES FOR CORRECTING AN ADJACENT BLOCK TRANSPOSITION AND A BURST DELETION

Next, we describe how to construct codes capable of correcting a single block transposition along with a single block deletion. For simplicity, we limit our attention to the case where the adjacent block transposition and the block deletion are both of the same size.

Similar to what was done in the previous section, we first outline the high level ideas behind the construction and the proof. We start with the special case when the block transposition and the block deletion are non-overlapping. Recall that for $r = n/b$ (where we tacitly assume that b divides n), it is convenient to represent the codeword $\mathbf{x} = (x_1, \dots, x_n)$ in the following manner:

$$\begin{bmatrix} x_1 & x_{b+1} & x_{2b+1} & \dots & x_{r(b-1)+1} \\ x_2 & x_{b+2} & x_{2b+2} & \dots & x_{r(b-1)+2} \\ \dots & \dots & \dots & \dots & \dots \\ x_b & x_{2b} & x_{3b} & \dots & x_n \end{bmatrix}. \quad (18)$$

Suppose that \mathbf{y} is the result of one adjacent block transposition and a block of deletions, both of length b . Note that the block deletion and adjacent block transposition has the equivalent effect of deleting one symbol from each row in the matrix representation of the codeword and swapping two adjacent symbols within each row.

One naive approach for constructing codes capable of correcting an adjacent block transposition and a block deletion is to use a 1-TD code on each of the b interleaved sequences in the matrix (18). Since a 1-TD code requires roughly $2 \log n$ bits of redundancy, this approach would result in a total redundancy of $2b \log n$ bits. In what follows, we describe a more involved approach that requires roughly $O((\log(b) + 8) \log n + (b^2 + 64b) \log \log n)$ bits of redundancy.

The proposed construction works as follows. We first ignore the adjacent block transposition and attempt to correct the block deletion using the method of the previous section. Clearly, with this approach we may (and will) perform erroneous correction. However, the ‘‘mis-correction’’ will have

a specific structure which may be exploited in the next step by using Tensor Product codes [24], to be described in this section.

To this end, we introduce the following notation. For a given word $\mathbf{x} \in \mathbb{F}_2^n$, let $\mathcal{B}_{BT,b}(\mathbf{x})$ denote the set of words that may be obtained from \mathbf{x} via one adjacent block transposition of length b (Recall from Section IV that we used $\mathcal{B}_{(T,\ell)}(\mathbf{x})$ to denote the set of words that may be obtained from at most ℓ adjacent transpositions in \mathbf{x}). The following simple example illustrates the newly introduced concept.

Example 11. Let $\mathbf{x} = (1, 0, 0, 0, 0, 0, 1, 1, 0) \in \mathbb{F}_2^9$. Here,

$$\mathcal{B}_{BT,3}(\mathbf{x}) = \{(1, 0, 0, 0, 0, 0, 1, 1, 0), (0, 0, 0, 1, 0, 0, 1, 1, 0), \\ (1, 0, 1, 1, 0, 0, 0, 1, 0), (1, 0, 0, 1, 1, 0, 0, 0, 0)\}.$$

Recall from Section IV that with respect to the size of the relevant error balls, the order in which a single adjacent transposition and a single deletion occur does not matter. The next example shows that, unfortunately, this property does not carry over to the case of adjacent block transpositions and block deletions.

Example 12. Let $\mathbf{x} = (1, 0, 0, 0, 0, 0, 1, 1, 0) \in \mathbb{F}_2^9$. Then, $(1, 1, 0, 1, 0, 0) \in \mathcal{B}_{BT,3}(\mathcal{B}_{D,3}(\mathbf{x}))$, but $(1, 1, 0, 1, 0, 0) \notin \mathcal{B}_{D,3}(\mathcal{B}_{BT,3}(\mathbf{x}))$. Similarly, let $\mathbf{y} = (1, 0, 1, 0, 0, 0, 1, 1, 0) \in \mathbb{F}_2^9$. Then, $(1, 0, 0, 0, 0, 0) \in \mathcal{B}_{D,3}(\mathcal{B}_{BT,3}(\mathbf{y}))$, but at the same time, $(1, 0, 0, 0, 0, 0) \notin \mathcal{B}_{BT,3}(\mathcal{B}_{D,3}(\mathbf{y}))$.

We would like to design codes that can correct block errors in either of the two orders, i.e., codes that can correct a block deletion followed by an adjacent block transposition *and simultaneously* correct an adjacent block transposition followed by a block deletion. Hence, we need to introduce one more notion of a set, which for a word $\mathbf{x} \in \mathbb{F}_2^n$ equals

$$\mathcal{B}_{BT \wedge D,b}(\mathbf{x}) = \bigcup_{t \leq b} \mathcal{B}_{BT,t}(\mathcal{B}_{D,t}(\mathbf{x})) \cup \mathcal{B}_{D,t}(\mathcal{B}_{BT,t}(\mathbf{x})).$$

We have the following useful claim.

Claim 6. For $\mathbf{x} \in \mathbb{F}_2^n$,

$$\mathcal{B}_{BT \wedge D,b}(\mathbf{x}) \subseteq \mathcal{B}_{D, \leq b}(\mathcal{B}_{(T, 2b^2)}(\mathbf{x})).$$

Using Claims 2 and 6, we can prove the following result.

Corollary 21. Suppose that $\mathbf{y} = (y_1, \dots, y_n) \in \mathcal{B}_{(T, 2b^2)}(\mathbf{x})$ where $\mathbf{x} \in \mathbb{F}_2^n$. Then, $|\sum_{i=1}^n ix_i - \sum_{i=1}^n iy_i| \leq 2b^2$.

The claims above allows us to generalize some of the results of Section IV. To this end, recall from the previous section that for $\mathbf{y} \in \mathbb{F}_2^{n-b}$, $\mathbf{v} \in \mathbb{F}_2^b$ and $k_I \in [n - b + 1]$, we used $I(\mathbf{y}, \mathbf{v}, k_I) \in \mathbb{F}_2^n$ to denote the vector obtained by inserting \mathbf{v} into \mathbf{y} at position k_I .

Claim 7. Let $\mathbf{v}_1, \mathbf{v}_2 \in \mathbb{F}_2^b$. Furthermore, suppose that $\mathbf{y} \in \mathbb{F}_2^{n-b}$, $w_1 = wt(\mathbf{v}_1) = wt(\mathbf{v}_2)$, and $i_1 < i_2$. Let $\mathbf{x} \in \mathcal{B}_{(T, 2b^2)}(I(\mathbf{y}, \mathbf{v}_1, i_1)) \in \mathbb{F}_2^n$, $w_2 = wt(x_{i_1+b}, \dots, x_{i_2+b-1})$, and $\mathbf{u} \in \mathcal{B}_{(T, 2b^2)}(I(\mathbf{y}, \mathbf{v}_2, i_2)) \in \mathbb{F}_2^n$. Then,

$$\sum_{i=1}^n iu_i - \sum_{i=1}^n ix_i = (i_2 - i_1)w_1 - bw_2 + \delta + \theta,$$

where $|\delta| < b^2$ and $|\theta| \leq 4b^2$.

Remark 3. The correction term θ arises as a consequence of allowing at most $2b^2$ adjacent transpositions to occur. The statement in Claim 7 then follows from Corollary 21.

As mentioned at the beginning of the section, we first attempt to correct the block deletion. Our approach to correcting the block of deletions will be similar to that described in the previous section, where we used VT-like codes combined with coding constraints needed to approximately estimate the weight and the location of the block of deletions. Afterwards, SVT codes will be used to attempt to accurately correct the deletions given the approximate starting location.

We first focus on the behavior of a single SVT decoder. Recall from the previous section that $D(\mathbf{x}, b, k_D)$ is the result of deleting b consecutive bits from \mathbf{x} starting at position k_D . Furthermore, let

$$\mathbf{y} = T(\mathbf{x}, k_T) = (x_1, \dots, x_{k_T-1}, x_{k_T+1}, x_{k_T}, x_{k_T+2}, \dots, x_n)$$

denote the word obtained by performing one adjacent transposition in \mathbf{x} starting at position k_T . The next lemma characterizes the behavior of a Shifted VT decoder when it is provided with a vector that has experienced a single deletion along with a single adjacent transposition. The proof of the result, which may be found in Appendix B, follows along the same lines as that of Lemma 9 and Corollary 10.

Lemma 22. Suppose that $\mathbf{x} \in SVT_{c,d}(n, 2P+2)$, where $c \in \mathbb{Z}_{2P+2}$, $d \in \mathbb{F}_2$, $\mathbf{y} \in D(T(\mathbf{x}, k_T), 1, k_D)$, and assume that we are given a \hat{k}_D such that $|\hat{k}_D - k_D| < P$. Then, there exists a decoder \mathcal{D}_{SVT} for $SVT_{c,d}(n, 2P+2)$ that can generate a vector $\mathbf{z} = I(\mathbf{y}, d_b, k'_D) \in SVT_{c,d}(n, 2P+2)$ for $d_b \in \mathbb{F}_2$ given \mathbf{y} and \hat{k}_D , such that $\mathbf{z} \in \mathcal{B}_{(T,2)}(\mathbf{x})$ and $|k'_D - \hat{k}_D| < P$.

Thus, similar to what we observed in the previous section, if a Shifted VT decoder is provided with a sufficiently accurate estimate of the location of the deletion, the decoder will either correct the deletion or introduce a miscorrection in the form of an additional transposition.

We first focus on the case where the blocks have odd length, and then extend it to the general case. The ideas behind the proofs represent a combination of the approaches from Sections IV and V.

Let $a \in \mathbb{Z}_{bn+5b^2}$, and suppose that \mathbf{C}, \mathbf{D} are defined as in (16). We start by introducing the following code:

$$\mathcal{C}_{TD,b}^{(1)}(n, a, \mathbf{C}, \mathbf{D}) = \left\{ \mathbf{x} \in \mathbb{F}_2^n : \sum_{i=1}^n ix_i \equiv a \pmod{bn + 5b^2}, \right. \\ \left. \mathbf{x} \in \text{Bal}(n, b), \text{ and } \forall i_2 \in [b], \forall i_1 \leq i_2, \text{ one has} \right. \\ \left. \mathbf{x}^{(i_1, i_2)} \in SVT_{c_{i_1, i_2}, d_{i_1, i_2}} \left(\left\lceil \frac{n - i_1 + 1}{i_2} \right\rceil, 2b^5 \log n + 2 \right) \right\}. \quad (19)$$

Let

$$\mathcal{C}_{TD,b}^{(1)}(n, a) := \left\{ \mathbf{x} \in \mathbb{F}_2^n : \sum_{i=1}^n ix_i \equiv a \pmod{bn + 5b^2}, \right. \\ \left. \mathbf{x} \in \text{Bal}(n, b) \right\}.$$

Observe that $\mathcal{C}_{TD,b}^{(1)}(n, a, \mathbf{C}, \mathbf{D}) \subseteq \mathcal{C}_{TD,b}^{(1)}(n, a)$. We show next that one can approximately determine the location of the block of deletions given $\mathcal{C}_{TD,b}^{(1)}(n, a)$. In this context, the next lemma is an analogue of Lemma 15, and its proof is given in the Appendix.

Lemma 23. *Let $\mathbf{v}_1, \mathbf{v}_2 \in \mathbb{F}_2^t$, $wt(\mathbf{v}_1) = wt(\mathbf{v}_2)$, $\mathbf{y} \in \mathbb{F}_2^{n-t}$, and suppose that $t \leq b$ is an odd number such that $b \geq 6$. For $i_1 < i_2$ and $i_2 - i_1 \geq b^4 \log n$, let $\mathbf{x} \in \mathcal{B}_{(T, 2b^2)}(I(\mathbf{y}, \mathbf{v}_1, i_1))$, $\mathbf{x} \in \mathcal{C}_{TD,b}^{(1)}(n, a)$ and $\mathbf{z} \in \mathcal{B}_{(T, 2b^2)}(I(\mathbf{y}, \mathbf{v}_2, i_2)) \in \mathbb{F}_2^n$. Then,*

$$\sum_{i=1}^n iz_i - \sum_{i=1}^n ix_i \not\equiv 0 \pmod{bn + 5b^2},$$

and so $\mathbf{z} \notin \mathcal{C}_{TD,b}^{(1)}(n, a)$.

Next, we define the code $\mathcal{C}_b^{Odd, B}(n, a, \mathbf{C}, \mathbf{D})$, which can correct any single block deletion and adjacent block transposition when the length of the blocks is odd. In order to define the code, we need to introduce tensor product codes. The following definition is adapted from [9].

Definition 24. *Given positive integers t_1 and t_2 , a binary error vector $\mathbf{e} = (e_1, e_2, \dots, e_n) \in \mathbb{F}_2^{mn}$ is called an $(n, m; t_1, t_2)$ error vector if each subvector \mathbf{e}_i , $1 \leq i \leq n$, is of length m , and*

- 1) $wt(\mathbf{e}) = |\{i : \mathbf{e}_i \neq \mathbf{0}\}| \leq t_1$, and
- 2) $\forall i, wt(\mathbf{e}_i) \leq t_2$.

We refer to a code $\mathcal{C} \subseteq \mathbb{F}_2^{mn}$ that is capable of correcting any $(n, m; t_1, t_2)$ error vector as an $\mathcal{C}(n, m; t_1, t_2)$ code. Suppose now that $(2b^5 \log n + b)$ divides n . We define the code $\mathcal{C}_b^{Odd, B}(n, a, \mathbf{C}, \mathbf{D})$ according to:

$$\mathcal{C}_b^{Odd, B}(n, a, \mathbf{C}, \mathbf{D}) = \left\{ \mathbf{x} \in \mathbb{F}_2^n : \mathbf{x} \in \mathcal{C}_{TD,b}^{(1)}(n, a, \mathbf{C}, \mathbf{D}), \right. \\ \left. \mathbf{x} \in \mathcal{C} \left(\frac{n}{2b^5 \log n + b}, 2b^5 \log n + b; 4, 4b \right) \right\}. \quad (20)$$

We have the following theorem, which relies on the result of Lemma 23.

Lemma 25. *Suppose that $\mathbf{x} \in \mathcal{C}_b^{Odd, B}(n, a, \mathbf{C}, \mathbf{D})$ and that $\mathbf{y} \in \mathcal{B}_{T \wedge D, b}(\mathbf{x})$, $\mathbf{y} \in \mathbb{F}_2^{n-t}$, where t is an odd integer, such that $t \leq b$ and $b \geq 6$. Then, there exists a decoder for $\mathcal{C}_b^{Odd, B}(n, a, \mathbf{C}, \mathbf{D})$ that can recover \mathbf{x} from \mathbf{y} .*

Proof: Since $\mathbf{y} \in \mathcal{B}_{T \wedge D, b}(\mathbf{x})$, we know from Claim 6 that $\mathbf{y} \in \mathcal{B}_{D, \leq b}(\mathcal{B}_{(T, 2b^2)}(\mathbf{x}))$. Therefore, there exists a vector $\mathbf{v}_1 \in \mathbb{F}_2^t$ and an index $k_D \in [n - t + 1]$ such that $\mathbf{x} \in \mathcal{B}_{(T, 2b^2)}(I(\mathbf{y}, \mathbf{v}_1, k_D))$ and $\mathbf{x} \in \mathcal{C}_b^{Odd, B}(n, a, \mathbf{C}, \mathbf{D})$.

Note that from the Shifted VT code constraints, we can determine $wt(\mathbf{v}_1)$ and hence produce a vector \mathbf{v}_2 with $wt(\mathbf{v}_1) = wt(\mathbf{v}_2)$. We may then generate a vector $\mathbf{z} \in \mathcal{B}_{(T, 2b^2)}(I(\mathbf{y}, \mathbf{v}_2, \hat{k}_D))$ such that $\mathbf{z} \in \mathcal{C}_{TD,b}^{(1)}(n, a)$. According to Lemma 23, we would have $|k_D - \hat{k}_D| < b^4 \log n$.

For each $\mathbf{y}^{(i, t)}$, where $i \leq t$, we have $\mathbf{y}^{(i, t)} \in \mathcal{B}_{(T, 1), D}(\mathbf{x}^{(i, t)})$. Suppose that $\mathbf{y}^{(i, t)} = D(T(\mathbf{x}^{(i, t)}, k_{T, i}), 1, k_{D, i})$ and that $k_{D, i} > k_{T, i} + 1$ (The case $k_{D, i} \leq k_{T, i} + 1$ can be analyzed similarly). Let $\mathbf{s}^{(i, t)} = D(\mathbf{x}^{(i, t)}, k_{D, i}) \in \mathcal{B}_D(\mathbf{x}^{(i, t)})$.

We use the decoder described in Lemma 22 to produce a vector $\mathbf{w}^{(i, t)}$, given the estimate $\hat{k}_{D, i} = \lceil \hat{k}_D / t \rceil$ and the vector $\mathbf{y}^{(i, t)}$ as inputs of the decoder. Suppose that $\mathbf{x}^{(i, t)} = I(\mathbf{s}^{(i, t)}, d_i, k_{D, i})$. Clearly, $|\hat{k}_{D, i} - k_{D, i}| < b^4 \log n$. According to Lemma 22, $\mathbf{w}^{(i, t)} = I(\mathbf{y}^{(i, t)}, d_i, k'_{D, i}) \in \mathcal{B}_{(T, 2)}(\mathbf{x}^{(i, t)})$, where $|k'_{D, i} - \hat{k}_{D, i}| < b^4 \log n$. Next, let $\mathbf{u}^{(i, t)} = T(\mathbf{w}^{(i, t)}, k_{T, i})$, where as before, $T(\mathbf{x}, k)$ denotes the word obtained by applying one adjacent transposition starting at position k in \mathbf{x} . Notice that $\mathbf{u}^{(i, t)} = I(\mathbf{s}^{(i, t)}, d_i, k'_{D, i})$, which implies that $\mathbf{u}^{(i, t)} \in \mathcal{B}_{(T, 1)}(\mathbf{x}^{(i, t)})$, since $\mathbf{w}^{(i, t)} \in \mathcal{B}_{(T, 2)}(\mathbf{x}^{(i, t)})$. Furthermore, since $\mathbf{x}^{(i, t)} = I(\mathbf{s}^{(i, t)}, d_i, k_{D, i})$, $\mathbf{u}^{(i, t)} \in \mathcal{B}_{(T, 1)}(\mathbf{x}^{(i, t)})$, and $|k_{D, i} - k'_{D, i}| < 2b^4 \log n$, there exists a $k'_{T, i}$ such that $|k'_{T, i} - k_{D, i}| < 2b^4 \log n + 1$ and $\mathbf{x}^{(i, t)} = T(\mathbf{u}^{(i, t)}, k'_{T, i})$.

Thus, we have at most two pairs of mismatched symbols between \mathbf{x}, \mathbf{w} , say at positions i_1, i_2, j_1, j_2 . Suppose, without loss of generality, that the errors in \mathbf{w} at positions i_1, i_2 are due to the adjacent block transposition and that errors at positions j_1, j_2 are due to the miscorrections associated with the Shifted VT decoders (which were described in the previous paragraph). Then, $|i_1 - i_2| \leq b$ and $|j_1 - j_2| \leq 2b^5 \log n + b$. This implies that \mathbf{w} and \mathbf{x} differ by at most a $(\frac{n}{2b^5 \log n + b}, 2b^5 \log n + b; 4, 4b)$ -type error. Since \mathbf{x} belongs to a $\mathcal{C}(\frac{n}{2b^5 \log n + b}, 2b^5 \log n + b; 4, 4b)$ -error correcting code, the proof follows. ■

We illustrate the encoding/decoding procedures with the following example.

Example 13. Suppose that

$$\mathbf{x} = (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \in \mathbb{F}_2^{21}$$

was transmitted and that $\mathbf{y} = (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \in \mathcal{B}_{D, 3}(\mathcal{B}_{BT, 3}(\mathbf{x}))$ was received instead. It is straightforward to check that $\sum_{i=1}^{21} ix_i \equiv 35 \pmod{108}$.

As the first step of decoding, we find a vector $\mathbf{v}_2 \in \mathbb{F}_2^3$ and another vector $\mathbf{z} = I(\mathbf{y}, \mathbf{v}_2, \hat{k})$ such that $wt(\mathbf{v}_2) = 3$ and $\sum_{i=1}^n iz_i \equiv 35 \pmod{108}$. There exists only one vector $\mathbf{z} = (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$ for which $\mathbf{v}_2 = (1, 1, 1)$ and $\hat{k} = 15$.

Notice that $\mathbf{x}^{(1, 3)} = (1, 0, 1, 1, 0, 1, 1)$ and that $\sum_{i=1}^7 ix_i^{(1, 3)} \equiv 5 \pmod{8}$. Thus, given that we know the value of the deleted bit, the parameter $\hat{k}_1 = 5$ (which is an estimate derived from \hat{k} , where $\hat{k}_1 = \lceil \frac{\hat{k}}{3} \rceil$), and $\mathbf{y}^{(1, 3)} = (0, 1, 1, 1, 0, 1)$, we may use the decoder described in Lemma 22 to generate $\mathbf{w}^{(1, 3)} = (0, 1, 1, 1, 0, 1)$. Similarly, as $\mathbf{w}^{(2, 3)} = (1, 1, 0, 0, 0, 1)$ and $\mathbf{w}^{(3, 3)} = (0, 1, 1, 1, 0, 1)$, one has $\mathbf{w} = (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$ (We have highlighted the positions where \mathbf{w} and \mathbf{x} differ). We can correct the remaining errors using a $(7, 3; 4, 2)$ -type code from Definition 24.

The following corollary follows from Lemma 25 and the well-known Gilbert-Varshamov bound.

Corollary 26. *Let $\mathcal{C}_b^{Odd, B}(n, a, \mathbf{C}, \mathbf{D})$ be as defined in (20). Let t be an odd positive integer such that $t \leq b$, with $b \geq 6$. Then, the code is a single transposition and block deletion correcting*

code. Furthermore, for any $n \geq 10$,

$$\begin{aligned} \log |\mathcal{C}_b^{Odd,B}(n, \mathbf{a}, \mathbf{C}, \mathbf{D})| &\geq \\ n - [\log(bn + 5b^2) + \frac{b(b+1)}{2} (\log(2b^5 \log n + 2) + 1) \\ &+ 8 \log n + 64b \log(2b^5 \log(n) + b) + 1]. \end{aligned}$$

An immediate consequence of the above corollary is that for $b = O(1)$, one has

$$\log |\mathcal{C}_b^{Odd,B}(n, \mathbf{a}, \mathbf{C}, \mathbf{D})| \geq n - [9 \log n + O(\log \log n)].$$

We are now ready to state the general code construction using the same approach as that described in the previous section. In particular, the next result proves the existence of a code capable of correcting any block of deletions and an adjacent block transposition; the redundancy of the construction is approximately $\log b (\log n + O(\log \log n)) + 8 \log n$ bits.

Define the codebook $\mathcal{C}_{TD,b}(n, \mathbf{a}, \vec{\mathbf{C}}, \vec{\mathbf{D}})$ according

$$\begin{aligned} \mathcal{C}_{TD,b}(n, \mathbf{a}, \vec{\mathbf{C}}, \vec{\mathbf{D}}) &= \left\{ \mathbf{x} \in \mathbb{F}_2^n : \right. \\ &\mathbf{x} \in \mathcal{C} \left(\frac{n}{2b^5 \log n + b}, 2b^5 \log n + b; 4, 4b \right), \\ &\forall j \in [\lceil \log b \rceil], \mathbf{x}^{(1, 2^{j-1})} \in \mathcal{C}_{TD, \tilde{b}}^{(1)}(\lceil \frac{n}{2^{j-1}} \rceil, a_j, \mathbf{C}_j, \mathbf{D}_j) \\ &\text{with } \tilde{b} = \max\{\lceil \frac{b}{2^{j-1}} \rceil, 6\} \}, \end{aligned}$$

with parameters $\mathbf{a} = (a_1, \dots, a_{\lceil \log b \rceil})$, $\vec{\mathbf{C}} = (\mathbf{C}_1, \dots, \mathbf{C}_{\lceil \log b \rceil})$, $\vec{\mathbf{D}} = (\mathbf{D}_1, \dots, \mathbf{D}_{\lceil \log b \rceil})$. The codes $\mathcal{C}_{TD, \tilde{b}}^{(1)}(\lceil \frac{n}{2^{j-1}} \rceil, a_j, \mathbf{C}_j, \mathbf{D}_j)$ are defined as in (19).

The following theorem follows from Lemma 25 and may be proved similarly as Theorem 19.

Theorem 27. Suppose that $\mathbf{x} \in \mathcal{C}_{TD,b}(n, \mathbf{a}, \vec{\mathbf{C}}, \vec{\mathbf{D}})$ is transmitted and that $\mathbf{y} \in \mathcal{B}_{BT \wedge D, b}(\mathbf{x})$ is received. Then, there exists a decoder for $\mathcal{C}_{TD,b}(n, \mathbf{a}, \vec{\mathbf{C}}, \vec{\mathbf{D}})$ capable of uniquely determining \mathbf{x} from \mathbf{y} .

Corollary 28. Let $\mathbf{x}, \mathbf{u} \in \mathcal{C}_{TD,b}(n, \mathbf{a}, \vec{\mathbf{C}}, \vec{\mathbf{D}})$ be defined as above. Then, for any $n \geq 50b$, $b \geq 6$, the code is a block transposition and deletion correcting code satisfying

$$\begin{aligned} \log |\mathcal{C}_{TD,b}(n, \mathbf{a}, \vec{\mathbf{C}}, \vec{\mathbf{D}})| &\geq \\ n - [\lceil \log b \rceil (\log(bn + 5b^2) + \frac{b(b+1)}{2} (\log(2b^5 \log n + 2) + 1)) \\ &+ 8 \log n + 64b \log(2b^5 \log(n) + b) + 1]. \end{aligned}$$

REFERENCES

- [1]
- [2] J. Bornholt, R. Lopez, D. M. Carmean, L. Ceze, G. Seelig, and K. Strauss, "A dna-based archival storage system," in *Proceedings of the Twenty-First International Conference on Architectural Support for Programming Languages and Operating Systems*. ACM, 2016, pp. 637–649.
- [3] J. Brakensiek, V. Guruswami, and S. Zbarsky, "Efficient low-redundancy codes for correcting multiple deletions," *arXiv preprint arXiv:1507.06175*, 2015.
- [4] E. Brill and R. C. Moore, "An improved error model for noisy channel spelling correction," in *Proceedings of the 38th Annual Meeting on Association for Computational Linguistics*. Association for Computational Linguistics, 2000, pp. 286–293.
- [5] L. Cheng, T. G. Swart, H. C. Ferreira, and K. A. Abdel-Ghaffar, "Codes for correcting three or more adjacent deletions or insertions," 2014.
- [6] G. M. Church, Y. Gao, and S. Kosuri, "Next-generation digital information storage in dna," *Science*, vol. 337, no. 6102, pp. 1628–1628, 2012.
- [7] D. Cullina and N. Kiyavash, "An improvement to levenshtein's upper bound on the cardinality of deletion correcting codes," *IEEE Transactions on Information Theory*, vol. 60, no. 7, pp. 3862–3870, 2014.
- [8] F. J. Damerau, "A technique for computer detection and correction of spelling errors," *Commun. ACM*, vol. 7, no. 3, pp. 171–176, Mar. 1964. [Online]. Available: <http://doi.acm.org/10.1145/363958.363994>
- [9] R. Gabrys, E. Yaakobi, and L. Dolecek, "Graded bit-error-correcting codes with applications to flash memory," *IEEE Transactions on Information Theory*, vol. 59, no. 4, pp. 2315–2327, 2013.
- [10] N. Goldman, P. Bertone, S. Chen, C. Dessimoz, E. M. LeProust, B. Sipos, and E. Birney, "Towards practical, high-capacity, low-maintenance information storage in synthesized dna," *Nature*, vol. 494, no. 7435, pp. 77–80, 2013.
- [11] M. Hagiwara, "A short proof for the multi-deletion error correction property of helberg codes," *IEICE Communications Express*, vol. 5, no. 2, pp. 49–51, 2016.
- [12] A. S. Helberg and H. C. Ferreira, "On multiple insertion/deletion correcting codes," *Information Theory, IEEE Transactions on*, vol. 48, no. 1, pp. 305–308, 2002.
- [13] A. Kulkarni and N. Kiyavash, "Nonasymptotic upper bounds for deletion correcting codes," *Information Theory, IEEE Transactions on*, vol. 59, no. 8, pp. 5115–5130, Aug 2013.
- [14] S. Kumar, K. Tamura, and M. Nei, "Mega3: integrated software for molecular evolutionary genetics analysis and sequence alignment," *Briefings in bioinformatics*, vol. 5, no. 2, pp. 150–163, 2004.
- [15] V. I. Levenshtein, "Binary codes capable of correcting deletions, insertions, and reversals," in *Soviet physics doklady*, vol. 10, no. 8, 1966, pp. 707–710.
- [16] F. Paluncic, T. G. Swart, J. H. Weber, H. C. Ferreira, and W. A. Clarke, "A note on non-binary multiple insertion/deletion correcting codes," in *2011 IEEE Information Theory Workshop*.
- [17] R. Roth, *Introduction to Coding Theory*. New York, NY, USA: Cambridge University Press, 2006.
- [18] F. Sala, R. Gabrys, C. Schoeny, and L. Dolecek, "Exact reconstruction from insertions in synchronization codes," *arXiv preprint arXiv:1604.03000*, 2016.
- [19] C. Schoeny, A. Wachter-Zeh, R. Gabrys, and E. Yaakobi, "Codes for correcting a burst of deletions or insertions," *arXiv preprint arXiv:1602.06820*, 2016.
- [20] L. J. Schulman and D. Zuckerman, "Asymptotically good codes correcting insertions, deletions, and transpositions," *IEEE transactions on information theory*, vol. 45, no. 7, pp. 2552–2557, 1999.
- [21] N. J. Sloane, "On single-deletion-correcting codes," *Codes and Designs, de Gruyter, Berlin*, pp. 273–291, 2002.
- [22] R. Varshamov and G. Tenen Holtz, "A code for correcting a single asymmetric error," *Automatica i Telemekhanika*, vol. 26, no. 2, pp. 288–292, 1965.
- [23] M. M. Vilenchik and A. G. Knudson, "Endogenous dna double-strand breaks: production, fidelity of repair, and induction of cancer," *Proceedings of the National Academy of Sciences*, vol. 100, no. 22, pp. 12 871–12 876, 2003.
- [24] J. Wolf, "On codes derivable from the tensor product of check matrices," *IEEE Transactions on Information Theory*, vol. 11, no. 2, pp. 281–284, 1965.
- [25] S. Yazdi, H. M. Kiah, E. R. Garcia, J. Ma, H. Zhao, and O. Milenkovic, "Dna-based storage: Trends and methods," *arXiv preprint arXiv:1507.01611*, 2015.
- [26] —, "A rewritable, random-access dna-based storage system," *Nature Scientific Reports*, <http://www.nature.com/articles/srep14138>, 2015.

APPENDIX A PROOF OF CLAIM 4

We first evaluate the probability that the first $M = b^4 \log n$ bits of \mathbf{x} have less than $M/2 - (M/3b)$ or more than $M/2 + (M/3b)$ ones. Let \mathbf{x} be a uniformly at random selected element from \mathbb{F}_2^n . For any $i \in [n]$, let X_i be the indicator random variable that takes the value one when $x_i = 1$ and zero otherwise. Then, (X_1, \dots, X_M) is an i.i.d random vector over $\{0, 1\}$. Invoking Hoeffding's inequality we obtain

$$P \left(\sum_{i=1}^M x_i \geq \frac{M}{2} + \frac{M}{3b} \right) = P \left(\sum_{i=1}^M x_i \geq \frac{M}{2} - \frac{M}{3b} \right) \leq e^{-\frac{2M}{9b^2}}.$$

Let

$$f(M, b) = e^{-\frac{2M}{9b^2}}.$$

Note that $f(M, b)$ is decreasing in M , since

$$\frac{\partial f(M, b)}{\partial M} = -\frac{2e^{-\frac{2M}{9b^2}}}{9b^2}.$$

Applying the union bound leads to

$$P(\mathbf{x} \notin \text{Bal}(n, b)) \leq 2n^2 f(b^4 \log n, b).$$

Thus, $|\text{Bal}(n, b)| \geq 2^n (1 - 2n^2 f(b^4 \log n, b))$ and so

$$\log |\text{Bal}(n, b)| \geq n + \log \left(1 - 2n^2 e^{-\frac{2}{9}b^2 \log e} \right).$$

APPENDIX B

PROOF OF DELETION CAPABILITY OF THE SHIFTED VT CODES

Here, we prove that the Shifted VT codes are able to determine the location of a deletion given a sufficiently accurate estimate of the location of the deletion. Recall from the previous exposition that a Shifted VT code, denoted $SVT_{c,d}(n, P)$, is defined as:

$$SVT_{c,d}(n, M) = \{ \mathbf{x} \in \mathbb{F}_2^n : \sum_{i=1}^n i x_i \equiv c \pmod{M}, \sum_{i=1}^n x_i \equiv d \pmod{2} \}.$$

The next two claims are straightforward to prove.

Claim 8. Let $\mathbf{y} \in \mathbb{F}_2^{n-1}$, $d_b \in \mathbb{F}_2$, and suppose that $\mathbf{x} = I(\mathbf{y}, d_b, i_1)$ and $\mathbf{u} = I(\mathbf{y}, d_b, i_2)$, where $i_2 > i_1$. Let $w = wt(\mathbf{y}_{i_1}, \dots, \mathbf{y}_{i_2-1})$. Then, for any $k \in [n]$,

$$\sum_{i=1}^n (k+i) u_i - \sum_{i=1}^n (k+i) x_i = (i_2 - i_1) d_b - w.$$

Claim 9. Let $\mathbf{y} \in \mathbb{F}_2^{n-1}$, $d_b \in \mathbb{F}_2$, and suppose that $\mathbf{x} = I(\mathbf{y}, d_b, i_1)$ and $\mathbf{u} = I(\mathbf{y}, d_b, i_2)$, where $i_2 > i_1$ so that $|i_2 - i_1| < P$. Then, for any $k \in [n]$ and $M \geq P$, it holds that

$$\sum_{i=1}^n (k+i) x_i \not\equiv \sum_{i=1}^n (k+i) u_i \pmod{M},$$

unless $\mathbf{x} = \mathbf{u}$.

As a consequence of the previous claim, we may prove the following lemma, which describes the deletion-correcting capabilities of Shifted VT codes.

Lemma 16. Suppose that $\mathbf{y} \in D(\mathbf{x}, 1, k_D)$, where $\mathbf{x} \in SVT_{c,d}(n, M)$ and where $M \geq 2P - 1$, $d_b \in \mathbb{F}_2$. Given \hat{k}_D is such that $|k_D - \hat{k}_D| < P$, there exists at most one possible value for k'_D and one possible value for d_b that jointly satisfy $I(\mathbf{y}, d_b, k'_D) \in SVT_{c,d}(n, M)$. In this setting, we have

$$I(\mathbf{y}, d_b, k'_D) = \mathbf{x}.$$

Proof: First, notice that we can determine the value of the bit deleted from \mathbf{x} from the constraint $\sum_{i=1}^n x_i \equiv d \pmod{2}$, since $\mathbf{x} \in SVT_{c,d}(n, M)$.

Let $d_b \in \mathbb{F}_2$ be the value of the deleted bit. Let $\mathbf{y}_1 = (y_1, \dots, y_{\hat{k}_D-P})$ and $\mathbf{y}_2 = (y_{\hat{k}_D+P-1}, \dots, y_{n-1})$. We have $(x_1, \dots, x_{\hat{k}_D-P}) = (y_1, \dots, y_{\hat{k}_D-P})$ and $(x_{\hat{k}_D+P}, \dots, x_n) = (y_{\hat{k}_D+P-1}, \dots, y_{n-1})$, since $|k_D - \hat{k}_D| < P$. Let

$$c' \equiv \sum_{i=1}^{\hat{k}_D-P} i y_i + \sum_{i=\hat{k}_D+P-1}^{n-1} (i+1) y_i \pmod{M}.$$

Then

$$\sum_{i=\hat{k}_D-P+1}^{\hat{k}_D+P-1} i x_i \equiv c - c' \pmod{M},$$

where c is, as we recall, one of the parameters of the SVT code. Let $\mathbf{u} = (x_{\hat{k}_D-P+1}, \dots, x_{\hat{k}_D+P-1})$ and observe that $\hat{\mathbf{y}} = (y_{\hat{k}_D-P+1}, \dots, y_{\hat{k}_D+P-2}) \in \mathcal{B}_D(\mathbf{u})$. Clearly, if \mathbf{u} is known then $\mathbf{x} = (\mathbf{y}_1, \mathbf{u}, \mathbf{y}_2)$. After a change of variables, we obtain

$$\sum_{j=1}^{2P-1} (\hat{k}_D - P + j) u_j \equiv c - c' \pmod{M}.$$

According to Claim 9, we can now recover \mathbf{u} given the previous equation and $\hat{\mathbf{y}}$. This proves the lemma. \blacksquare

In the following derivations, we once more make use of the vector

$$\mathbf{y} = T(\mathbf{x}, k_T) = (x_1, \dots, x_{k_T-1}, x_{k_T+1}, x_{k_T}, x_{k_T+2}, \dots, x_n).$$

Lemma 22. Suppose that $\mathbf{x} \in SVT_{c,d}(n, 2P+2)$, where $c \in \mathbb{Z}_{2P+2}$, $d \in \mathbb{F}_2$, $\mathbf{y} \in D(T(\mathbf{x}, k_T), 1, k_D)$, and assume that we are given a \hat{k}_D such that $|k_D - \hat{k}_D| < P$. Then, there exists a decoder \mathcal{D}_{SVT} for $SVT_{c,d}(n, 2P+2)$ that can generate a vector $\mathbf{z} = I(\mathbf{y}, d_b, k'_D) \in SVT_{c,d}(n, 2P+2)$ for $d_b \in \mathbb{F}_2$ given \mathbf{y} and \hat{k}_D , such that $\mathbf{z} \in \mathcal{B}_{(T,2)}(\mathbf{x})$ and $|k'_D - \hat{k}_D| < P$.

Proof: Suppose that $k_T + 1 < k_D$ (The case $k_T + 1 > k_D$ may be proved by applying the same argument to the reverses of the sequences).

Similarly as in the proof of Lemma 16, let $\mathbf{y}_1 = (y_1, \dots, y_{\hat{k}_D-P})$, $\mathbf{y}_2 = (y_{\hat{k}_D+P-1}, \dots, y_{n-1})$, and $\mathbf{u} = (x_{\hat{k}_D-P+1}, \dots, x_{\hat{k}_D+P-1})$.

Also, let $\hat{\mathbf{y}} = (y_{\hat{k}_D-P+1}, \dots, y_{\hat{k}_D+P-2})$.

First, we consider the case when $k_T \in \{\hat{k}_D - P + 1, \dots, \hat{k}_D + P - 1\}$. Then, we have $\hat{\mathbf{y}} \in \mathcal{B}_{(T,1),D}(\mathbf{u})$. Letting c' be defined as in the proof of Lemma 16, we can show that

$$\sum_{j=1}^{2P-1} (\hat{k}_D - P + j) u_j \equiv c - c' \pmod{2P+2},$$

and can hence recover the value of the deleted bit from $\sum_{j=1}^{2P-1} u_j \pmod{2}$. The claimed result now follows from Corollary 10.

Next, suppose that $k_T < \hat{k}_D - P + 1$. We assume that k_D is not in the first or last run of the vector \mathbf{y} (The case when k_D is in the first or last run can be proved similarly, but is slightly more technical). Let k_U be the largest index such that

both $y_{k_U} = y_{k_D}$ and y_{k_U}, y_{k_D} belong to the same run. Similarly, let k_L be the smallest index such that both $y_{k_L} = y_{k_D}$ and y_{k_L}, y_{k_D} belong to the same run.

Suppose that $d_b \in \mathbb{F}_2$ is the bit deleted from \mathbf{x} . If $x_{k_T} = x_{k_D}$, set $\mathbf{z} = T(I(\mathbf{y}, d_b, k_D), k_L - 1)$, and notice that $\mathbf{z} = T(I(\mathbf{y}, d_b, k_D), k_L - 1) = I(\mathbf{y}, d_b, k_L - 1) \in SVT_{c,d}(n, 2P+2)$ and $\mathbf{z} = T(T(\mathbf{x}, k_L - 1), k_T)$. Clearly, $\mathbf{z} \in \mathcal{B}_{(T,2)}(\mathbf{x})$ and from Lemma 16, $\mathbf{z} = I(\mathbf{y}, d_b, k_L - 1)$ is unique. The case $x_{k_T} \neq x_{k_D}$ may be handled similarly. ■

APPENDIX C PROOF OF COROLLARY 18

The claim that for $\mathbf{x}, \mathbf{u} \in \mathcal{C}_b^{Odd}(n, a, \mathbf{C}, \mathbf{D}) \subseteq \mathbb{F}_2^n$, one has $\mathcal{B}_{D,t}(\mathbf{x}) \cap \mathcal{B}_{D,t}(\mathbf{u}) = \emptyset$ follows immediately from Theorem 17.

Regarding the claim about the code redundancy, we consider the set of “balanced” words $Bal(n, b)$ as defined in (12) and apply an averaging argument which involves the parameters $a, c_{i_1, i_2}, d_{i_1, i_2}$. Then,

$$|\mathcal{C}_b^{Odd}(n, a, \mathbf{C}, \mathbf{D})| \geq \frac{|Bal(n, b)|}{(bn + b^2) \prod_{i_2=1}^b \prod_{i_1=1}^{i_2} 2(2b^5 \log n)}.$$

Taking the logarithms of both sides provides the claimed result.

APPENDIX D PROOF OF COROLLARY 20

The claim that for $\mathbf{x}, \mathbf{u} \in \mathcal{C}_b(n, a, \vec{\mathbf{C}}, \vec{\mathbf{D}}) \subseteq \mathbb{F}_2^n$, $\mathcal{B}_{D, \leq b}(\mathbf{x}) \cap \mathcal{B}_{D, \leq b}(\mathbf{u}) = \emptyset$ follows from Theorem 19. From the constraints in (17), if $\mathbf{x} \in \mathcal{C}_b(n, a, \vec{\mathbf{C}}, \vec{\mathbf{D}})$, then for $j \in [\lceil \log b \rceil]$, we have

$$\mathbf{x}^{(1, 2^{j-1})} \in \mathcal{C}_b^{Odd}(\lceil \frac{n}{2^{j-1}} \rceil, a_j, \mathbf{C}_j, \mathbf{D}_j),$$

where $\tilde{b} = \max\{\lceil b/2^{j-1} \rceil, 5\}$. Thus, $\mathbf{x} \in Bal(\lceil n/2^{j-1} \rceil, \tilde{b})$. Clearly, from (12), we have $|Bal(\lceil n/2^{j-1} \rceil, \tilde{b})| \geq |Bal(\lceil n/2^{j-1} \rceil, b)|$. Invoking the proof of Claim 4 with $b \geq 5$, and applying the union bound, we arrive at the bound

$$\begin{aligned} P(\exists j \in [\lceil \log b \rceil], \mathbf{x}^{(1, 2^{j-1})} \notin Bal(\lceil \frac{n}{2^{j-1}} \rceil, \tilde{b})) \\ \leq \lceil \log b \rceil 2 \left(\frac{n}{b} \right)^{2 - \frac{2b^2}{27 \log_e(2)}} \\ \leq \frac{1}{2} \end{aligned}$$

which holds whenever $n \geq 50b$. Thus, using similar arguments as those invoked in the proof of Corollary 18, we have

$$\begin{aligned} |\mathcal{C}_b^{Odd}(n, a, \mathbf{C}, \mathbf{D})| &\geq \frac{2^{n-1}}{\left((bn + b^2) \prod_{i_2=1}^b \prod_{i_1=1}^{i_2} 2(2b^5 \log n) \right)^{\lceil \log b \rceil}}. \end{aligned}$$

APPENDIX E PROOF OF LEMMA 23

We repeat the same steps of the proof used to establish Lemma 15.

Let $w_1 = wt(\mathbf{v}_1) = wt(\mathbf{v}_2)$ and $w_2 = wt(x_{i_1+t}, \dots, x_{i_2+t-1})$. Now according to Claim 7,

$$\sum_{i=1}^n i z_i - \sum_{i=1}^n i x_i = (i_2 - i_1) w_1 - t w_2 + C + D$$

and so in what follows we focus on showing that

$$B w_1 + C + D \not\equiv t w_2 \pmod{bn + 5b^2} \quad (21)$$

for $B = i_2 - i_1 \geq b^4 \log n$.

Since $\mathbf{x} \in \mathcal{C}_{TD,b}^{(1)}(n, a)$, we have $\mathbf{x} \in Bal(n, b)$ and so

$$\frac{B}{2} - \frac{B}{3b} < \sum_{i=i_1+t}^{i_2+t-1} x_i < \frac{B}{2} + \frac{B}{3b}$$

follows from (12). Thus, since $t \leq b$

$$\frac{Bt}{2} - \frac{B}{3} < t w_2 < \frac{Bt}{2} + \frac{B}{3}.$$

Notice that since t is odd, and since $w_1 = (t+k)/2$, $-b \leq k \leq b$, k has to be odd. Thus, we have

$$B w_1 + C + D = \frac{Bb}{2} + k \frac{B}{2} + C + D,$$

where $k \neq 0$. We will prove the result for the case when k is positive (The case when k is negative may be proved using the same argument). For $k \geq 1$, we have

$$B w_1 + C + D \geq \frac{Bt}{2} + \frac{B}{2} - b^2 - 4b^2.$$

Since $B \geq b^4 \log n$ and $b \geq 6$, one has

$$B w_1 + C + D \geq \frac{Bt}{2} + \frac{B}{2} - 5b^2 > \frac{Bt}{2} + \frac{B}{3} > t w_2,$$

so that (21) holds.

APPENDIX F PROOF OF COROLLARY 26

From (20), we may write

$$\begin{aligned} \mathcal{C}_b^{Odd, B}(n, a, \mathbf{C}, \mathbf{D}) &= \left\{ \mathbf{x} \in \mathbb{F}_2^n : \mathbf{x} \in \mathcal{C}_{TD,b}^{(1)}(n, a, \mathbf{C}, \mathbf{D}), \right. \\ &\quad \left. \mathbf{x} \in \mathcal{C} \left(\frac{n}{2b^5 \log n + b}, 2b^5 \log n + b; 4, 4b \right) \right\}. \end{aligned}$$

Repeating the same arguments as invoked in Corollary 18, we have

$$|\mathcal{C}_{TD,b}^{(1)}(n, a, \mathbf{C}, \mathbf{D})| \geq \frac{|Bal(n, b)|}{(bn + 5b^2) \prod_{i_2=1}^b \prod_{i_1=1}^{i_2} 2(2b^5 \log n + 2)},$$

and so

$$\begin{aligned} n - |\mathcal{C}_{TD,b}^{(1)}(n, a, \mathbf{C}, \mathbf{D})| &\leq \log(bn + 5b^2) + \frac{b(b+1)}{2} \\ &\quad (\log(2b^5 \log n + 2) + 1) + 1. \end{aligned}$$

The parity check matrix of a $\mathcal{C}(n/(2b^5 \log n + b), 2b^5 \log n + b; 4, 4b)$ -type code can be formed as follows [9]. Let H_2 be a parity-check matrix of a binary code \mathcal{C}_2 with Hamming distance $8b+1$ and of length $2b^5 \log n + b$. Also, let H_q be a parity-check matrix of a non-binary code \mathcal{C}_q that has minimum Hamming distance 9 and length $n/(2b^5 \log n + b)$. Then a parity-check matrix for a $\mathcal{C}(n/(2b^5 \log n + b), 2b^5 \log n + b; 4, 4b)$ -type code can be formed by taking the tensor product $H_q \otimes H_2$.

Applying the Gilbert-Varshamov bound, we obtain $n - \log |\mathcal{C}_2| \leq 8b \log(2b^5 \log n + b)$ and so

$$n - \log |\mathcal{C}_q| \leq 64b \log(2b^5 \log n + b) + 8 \log n.$$

Using the same averaging arguments as before establishes the claim in the corollary.